informática y DERECHO 4

DIRECTOR: VALENTÍN CARRASCOSA LÓPEZ



III CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO

ACTAS

(VOLUMEN I)

UNED
Centro Regional de Extremadura

ARANZADI
EDITORIAL

informática y DERECHO 4

DIRECTOR: VALENTÍN CARRASCOSA LÓPEZ

SOBRE LA EDICIÓN DIGITAL 2012

La presente edición es el resultado de un acuerdo de colaboración entre la *Federación Iberoamericana de Asociaciones de Derecho e Informática* (FIADI) y el *Instituto Chileno de Derecho y Tecnologías* (ICDT), formalizado en octubre de 2011 en la ciudad de Buenos Aires, en que se decidió re-editar digitalmente la que es la primera publicación periódica de habla castellana en Derecho Informático: **Informática y Derecho**, **Revista Iberoamericana de Derecho Informático**, que vio la luz en el año 1992 en el Centro Regional de Extremadura de la UNED de la ciudad de Mérida (España) bajo la dirección del Prof. Dr. Valentín Carrascosa López, y que dejó de publicarse tras una década de fructífera labor.

El objetivo final de esta nueva edición digital, ahora a cargo del *Instituto Chileno de Derecho y Tecnologías*, es rescatar los trabajos, investigaciones e ideas aparecidos en las páginas de esta revista académica para su libre consulta por futuras generaciones de docentes, investigadores y estudiantes, como modo de contribuir no solo con la preservación de la cultura jurídica, sino también aportar conocimiento a la historia de las ideas y rescatar la labor de los pioneros en temas de Derecho y Tecnologías en Iberoamérica.





informática y DERECHO 4

DIRECTOR: VALENTÍN CARRASCOSA LÓPEZ

ARANZADI
EDITORIAL

EDICION ORIGINAL IMPRESA

Universidad Nacional de Educación a Distancia
Centro Regional de Extremadura – Mérida
Depósito Legal: NA 127/1994
ISBN 88861 - 02 - 8 (Obra completa)
ISBN 88861 - 00 - 1 (Tomo IV)

EDICIÓN DIGITAL 2012

Instituto Chileno de Derecho y Tecnologías
c/ Melchor Concha y Toro 187
7520312 Providencia,
Santiago de Chile
Web: http://www.icdt.cl

SUMARIO

Página

PROLOGO 19

PRESENTACION:

Comité de Honor 27
Instituciones Organizadoras 30
Instituciones y Empresas Copatrocinadoras 30
Comité Científico y Organizador 31
Reglamento para la presentación de comunicaciones 33
Expositores 35
Talleres 35
Desarrollo del Congreso:
Sesión Inaugural 37
Sesiones Ordinarias 37
Sesión de Clausura 39
Exposición 40
Talleres 40
Actos Sociales 40
Programa 42

MENSAJE DEL DIRECTOR GENERAL DE LA UNESCO 52

CONFERENCIA INAUGURAL 55

ACTAS (VOLUMEN I)

SESION I
MESA N.º 1.–PROTECCION DE DATOS I
(ASPECTOS GENERALES)

ALENDE, JORGE OSCAR
«Informática: El abuso de su poder» 73

Página

BLÁZQUEZ ANDRÉS, M.ª CONSUELO y CARRASCOSA LÓPEZ, VALENTÍN
«Intimidad personal y limitaciones» 85

DE JULIOS CAMPUZANO, ALFONSO
«Derecho a la intimidad y publicidad de datos personales de carácter patrimonial» 91

DE VAL ARNAL, JOSÉ JESÚS
«La presunción de inocencia y el deber de colaboración con la inspección de trabajo. Derecho de acceder a los archivos informáticos». 97

FERNANDO PABLO, MARCOS MATIAS
«Administración Pública, Informática y ciudadano: perspectiva general» 109

MARTÍN BERNAL, JOSE MANUEL y MARTÍN GARCÍA, PILAR
«Intimidad y libertades» 119

MONTERO, ETIÉNNE
«Las obligaciones y responsabilidades del «titular» de un fichero de datos nominativos en cuanto a la cualidad de su producto» .. 129

ORZABAL, JOSEFINA C.
«Bases de datos, privacidad y responsabilidad civil» 137

SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, MANUEL
«La transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas» 145

SÁNCHEZ JIMÉNEZ, ENRIQUE
«Los derechos humanos de la 3.ª generación: la libertad informática» 165

COLOQUIOS *Mesa 1* 175

SESION II

MESA N.º 2.–PROTECCION DE DATOS II
(Análisis de la LORTAD)

ARROYO YANES, LUIS MIGUEL
«La cancelación de datos personales en ficheros de titularidad pública en el proyecto de LORTAD en España» 181

CASTILLO JIMÉNEZ, M.ª CINTA
«Análisis comparativo entre la Ley 10/91 portuguesa y el proyecto de LORTAD de nuestro país» 193

GAYO SANTA CECILIA, MARÍA EUGENIA
«Garantías del ciudadano ante la LORTAD: Posibles vías de defensa y protección de sus derechos fundamentales» 201

OROZCO PARDO, GUILLERMO
«Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal» 209

PÉREZ LUÑO, ANTONIO E.
«La protección de datos personales en España: presente y futuro». 235

RAMIRO LOZANO, INMACULADA y CARRASCOSA LÓPEZ, VALENTÍN
«La protección de datos personales en la Península Ibérica» 247

SANTAMARÍA IBEAS, JOSÉ JAVIER
«La LORTAD: breve análisis de sus antecedentes» 261

MESA N.º 3.–PROTECCION DE DATOS III
(Situación Internacional)

ASPAS ASPAS, JOSÉ M.ª
«El Derecho a la Autodeterminación informativa en la Ley Portuguesa de Protección de Datos de 1991. Sujetos, contenidos y garantías» 277

DE CARTOLANO, SILVIA C.
«Reforma de la constitución de Río Negro: necesidad de introducir el tema "Informática y protección de datos personales"»..... 293

HEREDERO HIGUERAS, MANUEL
«La protección de los datos de carácter personal registrados en soporte informatizado con fines estadísticos en el Derecho español» 299

MARTÍN ONCINA, JOSÉ IGNACIO
«La protección de datos informáticos en el derecho comparado» ... 313

RIPOL CARULLA, SANTIAGO
«Valoración española del proyecto de directiva comunitaria sobre

Página

protección de datos (contribución al estudio de la noción de posición nacional)» 321

SÁENZ GIL, RUBÉN
«Protección de las personas respecto al tratamiento automatizado de datos personales. Normativa Europea. Proyecto de Ley Española» 331

SÁNCHEZ BRAVO, ALVARO AVELINO
«El tratamiento automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: su protección» 341

TIRADO ROBLES, M.ª CARMEN
«La Comunidad Europea ante la Circulación de Datos Personales. Su protección jurídica» 351

COLOQUIOS: *Mesas 2 y 3* 363

SESION III

MESA N.º 4.–CONTRATACION INFORMATICA Y PROTECCION DEL SOFTWARE

AMOROSO FERNÁNDEZ, YARINA
«La informática en Cuba. Algunas consideraciones acerca de la protección y comercialización del Software. Régimen de protección de los datos» 381

BAUZA REILLY, MARCELO
«Protección Jurídica del Software en el Derecho Uruguayo» 393

BENITO-BUTRÓN OCHOA, JUAN C.
«Contrato de arrendamiento sobre bienes informáticos» 401

DARÍO BERGEL, SALVADOR
«Responsabilidad Civil derivada de la informática» 407

CASTRO FERNÁNDEZ, JUAN DIEGO y CASTRO CARVAJAL, PATRICIA
«La protección legal del "Software" en Costa Rica» 417

CORREA, CARLOS M.ª
«El Derecho Informático en el proyecto de acuerdo TRIPs de la Rueda Uruguay» 425

MIER y CONCHA SEGURA, JORGE
«Los Virus Computacionales como medio de Protección del Software» 435

Página

VAN HOUTTE, PAUL
«El Seguro de Responsabilidad Civil Profesional de los Informáticos» 445

MESA N.º 5.–DELITOS INFORMATICOS

ALASTUEY DOBÓN, M.ª DEL CARMEN
«Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial» 453

DEL PESO NAVARRO, EMILIO
«Prevención Versus Fraude: la Auditoría Informática» 465

GALLARDO ORTIZ, MIGUEL
«Criptología; Seguridad Informática y Derecho. Leyes del Ciberespacio» 473

GÓMEZ PERALS, MIGUEL
«Los Delitos Informáticos en el Derecho Español» 481

GUTIÉRREZ FRANCÉS, M.ª LUZ
«La criminalidad defraudatoria por medios informáticos en el Anteproyecto de Nuevo Cádigo Penal de 1992» 497

JIJENA LEIVA, RENATO JAVIER
«La criminalidad informática: situación del lege data y lege ferenda en Chile» 507

TÉLLEZ VALDÉS, JULIO
«Aspectos legales de los virus informáticos» 515

COLOQUIOS: *Mesas 4 y 5* 527

SESION IV

MESA N.º 6.–REGULACION JURIDICA DE LA INFORMATICA Y LAS TELECOMUNICACIONES

DE PAZ ARIAS, JOSÉ MARÍA
«Utilización de la Informática en la Detección de comportamientos irregulares en los Mercados de Valores» 541

GIMENO FELIÚ, JOSÉ MARÍA y TENA PIAZUELO, VITELIO M.ª
«El Derecho Comunitario de las Telecomunicaciones» 549

Página

GONZALES AGUILAR, AUDILIO
«EDI (Echange Data Informatics): Desafío de una nueva práctica» 555

PÁEZ MAÑA, JORGE y TRIVIÑO ACUÑA, EVA
«Flujo internacional de información» 569

RAMOS SIMÓN, LUIS FERNANDO
«Notas sobre las nuevas tecnologías de la información y sus relaciones con el Derecho a la Comunicación» 579

MESA N.º 7.–IMPACTO DE LA INFORMATICA EN EL DERECHO

BLÁZQUEZ ANDRÉS, M.ª CONSUELO y CARRASCOSA LÓPEZ, VALENTÍN
«El Derecho de la Informática en la formación de juristas e informáticos» 589

DE NO-LOUIS Y CABALLERO, EDUARDO
«El Working-House informático o tele-trabajo» 593

DURAND ALCÁNTARA, CARLOS y RIVERA SALGADO, DANIEL V.
«Derecho consuetudinario indígena y la informática» 605

GALINDO AYUDA, FERNANDO
«"Informática y derecho" como asignatura para informáticos» 613

GONZÁLEZ-TABLAS Y SASTRE, RAFAEL
«Aplicaciones informáticas en la enseñanza del derecho: reflexiones y métodos de calificación automática» 633

LÓPEZ-IBOR MAYOR, VICENTE y GARCÍA DELGADO, SONSOLES
«Situación del derecho informático en España y en Europa: algunas consideraciones» 643

SERRADILLA SANTOS, M.ª PAZ; TRINIDAD NÚÑEZ, AURELIA y VELÁZQUEZ RODRÍGUEZ, TERESA
«Implicaciones de la informática en el ámbito laboral» 657

COLOQUIOS *Mesa 7* 677

ACTAS (VOLUMEN II)

SESION V

MESA N.º 8.–BASES DE DATOS JURIDICAS

CASTRO FERNÁNDEZ, JUAN DIEGO
«Base de datos constitucionales» 719

CORDERO ALVARADO, JUVENTINO
«Base de datos. Elemento indispensable para la libertad profesional, un caso de México» 725

DE CARTOLANO, SILVIA C.
«Banco de datos jurídicos» 731

DÍAZ DEL BARCO, HORACIO
«La base de datos IBERLEX del Boletín Oficial del Estado en CD-ROM» 737

LÓPEZ-IBOR MAYOR, VICENTE y GARCÍA DELGADO, SONSOLES
«La industria de las bases de datos y su aplicación al derecho: experiencias de la producción y distribución en el sector eléctrico español» 745

LÓPEZ-MUÑÍZ DE MENDIZÁBAL, BLANCA y VÁZQUEZ DOCAMPO, RAMÓN
«MAP LEXTER: Sistema de bases de datos jurídicas integradas sobre administraciones territoriales» 765

ORLANDO, MÓNICA y MAZET, GUY
«La Condición de Originalidad en los Bancos de Datos» 775

RICO BONILLA, INMACULADA
«El impacto de la informática en el lenguaje jurídico» 781

SUÁREZ MARTÍNEZ, DIEGO F. y ALENDE, JORGE OSCAR
«Sistema argentino de informática jurídica» 789

MESA N.º 9.–HIPERTEXTO E INFORMATICA LEGISLATIVA

AMOROSO FERNÁNDEZ, YARINA
«Legislar asistido por computadoras» 801

AMOROSO FERNÁNDEZ, YARINA
«Proyecto MENJUR: una alternativa válida para el perfeccionamiento del ordenamiento jurídico cubano» 815

Página

BAUZA REILLY, MARCELO
«La información jurídica: adecuado análisis, correcto procesamiento y buena recuperación» 825

DOMÍNGUEZ LUIS, JOSÉ A.
«Informática y técnica legislativa» 833

GONZALES AGUILAR, AUDILIO
«Hipertextos y Derecho» 851

LIMA TORRADO, JESÚS y ROVETTA KLYVER, FERNANDO
«Hipertexto y Derecho» 861

RAMÍREZ HUAMAN, JORGE L.
«El aspecto de la interpretación jurídica en el tema de los sistemas expertos aplicados al Derecho» 869

COLOQUIOS *Mesas 8 y 9* 877

SESION VI

MESA N.º 10.–INFORMATICA DECISIONAL Y SISTEMAS EXPERTOS

CAMMELLI, ANTONIO y SOCCI, FIORENZA
«Lexis: un sistema experto jurídico para la interpretación y la redacción de las normas» 897

CORDERO ALVARADO, JUVENTINO; BERMÚDEZ GÓMEZ, SALVADOR
«Bases de conocimiento en la consulta legal» 903

DÁVARA RODRÍGUEZ, MIGUEL ANGEL
«Introducción a los sistemas expertos» 909

LASALA CALLEJA, PILAR; LEKUONA AMIANO, ALBERTO; LACRUZ CASAUCAU, BEATRIZ; AGUARÓN JOVEN, JUAN y PEINADO VISANZAY, ROSARIO
«Generación de una base de casos para un sistema experto que razona por analogías» 921

LÓPEZ-IBOR MAYOR, VICENTE y MARTÍNEZ PEÑALVER, LUIS OLIVIÉ
«Sistemas de ayuda a la decisión en el ámbito jurídico de la contratación» 935

Página

LÓPEZ RODRÍGUEZ MUÑÍZ DE MENDIZÁBAL, BLANCA
«Sistemas expertos: viabilidad de su aplicación al derecho» 957

MORENO, JOSÉ ANGEL
«Sistemas de ayuda a la decisión en las administraciones públicas» .. 969

PÉREZ DE LA CRUZ, JOSÉ LUIS; AURIOLES MARTÍN, ADOLFO; BELMONTE MARTÍNEZ, M.ª VICTORIA y HERNÁNDEZ PASCUAL, AMPARO
«Un sistema experto en derecho cambiario» 977

MESA N.º 11.–INFORMATICA JUDICIAL

BRENNA, RAMÓN GERÓNIMO y BIELSA, RAFAEL ANTONIO
«Organización de la justicia y nuevas tecnologías» 989

CAMPANELLA DE RIZZI, ELENA M.
«Informática judicial documental y de gestión en el poder judicial de la nación de la República Argentina» 1039

CARRASCOSA LÓPEZ, VALENTÍN
«La gestión automatizada en el ámbito de la Justicia Española» .. 1045

DÓVALO TABOADA, JOSÉ y ALIE COLL, ENRIQUE
«Evolución en el período 1989-1992, de los proyectos de informatización de la Administración de Justicia expuestos en el I y II Congresos (Santo Domingo y Guatemala)» 1075

ELORZA URBINA, MIKEL
«Propuesta de modernización de la Administración de Justicia. El plan de informatización de la Administración de Justicia de Euskadi» 1083

GARCERÁN CORTIJO, ANTONIO
«Comunicaciones Informáticas. Los procuradores y la administración» 1093

GONZÁLEZ RODRÍGUEZ, FRANCISCO PEDRO
«La informática en la Administración de Justicia» 1101

GUERRA GIMENO, ANTONIO y SÁNCHEZ GUIU, IÑAKI
«Informatización de la Administración de Justicia en Euskadi. Una experiencia concreta: la gestión del orden jurisdiccional civil» 1111

HURTADO, CARLOS FELIPE
«Nuevas tecnologías en el proceso y en el servicio de la Administración de Justicia» 1135

MUNICIO SANZ, GREGORIO
«La informática y el procedimiento administrativo de apremio» 1143

OTEROS FERNÁNDEZ, MANUEL
«El Secretario judicial y la informatización integral de los Juzgados de primera instancia» 1153

COLOQUIOS *Mesas 10 y 11* 1165

SESION VII

MESA N.º 12.–INFORMATICA JURIDICA Y REGISTRAL

ALIE COLL, ENRIQUE y DÓVALO TABOADA, JOSÉ
«Integración de la gestión informática judicial en el área Iberoamericana» 1179

AMENTA, PAULO MARCO y FERNÁNDEZ, RUBÉN IGNACIO
«Informatización de solicitudes mineras de la provincia de Tucuman República Argentina» 1189

ARENA, ALICIA; BIELSA, RAFAEL; VILAS, JORGE y GUTIÉRREZ, ANÍBAL
«Metodología para la Reconversión de un Sistema Público Automatizado de Información Jurídica» 1195

BUENO MALUENDA, CRISTINA
«La nueva gestión tributaria local» 1209

COLLADO VELÁZQUEZ, JUAN CARLOS
«Automatización del piso de remates en la bolsa mexicana de valores» 1219

COMISIÓN DE INFORMÁTICA JURÍDICA DEL COLEGIO PÚBLICO DE ABOGADOS DE LA CAPITAL FEDERAL DE LA REPÚBLICA
«La informática aplicada al derecho: presente y futuro, a través del accionar del Colegio Público de Abogados de la Capital Federal de la República Argentina» 1223

DE CARTOLANO, SILVIA C.
«Registro de la propiedad inmueble. Necesidad de su informatización» 1233

JOVER I PADRO, JOSEP
«El proyecto de colegios de Abogados de Barcelona en el ámbito de la informática jurídica» 1239

OROS y MURUZÁBAL, MIQUEL
«La informatización de la medicina forense en Cataluña. Ventajas conseguidas en la administración de justicia tras cinco años de implatantación» 1247

RAMÍREZ HUAMAN, JORGE LUIS
«Informática y Administración de Justicia en el Perú: apuntes a propósito de un proyecto» 1257

RUANI, HUMBERTO FÉLIX
«Función integradora de la informática jurídica en las distintas ramas del Derecho Iberoamericano: aporte de reciente ley argentina de transferencia electrónica de datos de la Cámara de casación penal y del SAIJ» 1265

MESA N.º 13.–PROCESO INFORMATIZADO Y DERECHO DE PRUEBA

ALVAREZ-CIENFUEGOS SUÁREZ, JOSÉ MARÍA
«Las obligaciones concertadas por medios informáticos y la documentación electrónica de los actos jurídicos» 1273

BAUZA REILLY, MARCELO
«Aperturas del Derecho de la prueba en Uruguay en materia de nuevas tecnologías de información» 1299

CASTRO FERNÁNDEZ, JUAN DIEGO
«El habeas data en Costa Rica» 1313

COSENTINO, GUILLERMO R.
«Informática y Reforma» 1319

DE ZULUETA CEBRIÁN, CARLOS
«El procurador en el Proceso Informatizado» 1331

FERREYROS SOTO, CARLOS
«Automatización de la instrucción penal ordinaria en el Perú: análisis y proposiciones» 1341

LLACER RUBIO, ENRIQUE; LUNA HUERTAS, PAULA y RUIZ DEL CASTILLO, JOSÉ CARLOS
«Ultimas tecnologías en soportes electrónicos y su utilidad para los profesionales del derecho» 1353

LÓPEZ-MUÑÍZ GOÑI, MIGUEL
«El proceso informatizado Multimedia» 1361

VAQUERO CARBALLO, JESÚS
«La informática en los centros penitenciarios» 1369

COLOQUIOS *Mesas 12 y 13* 1381

SESION VIII

MESA N.º 14.–PANORAMA IBEROAMERICANO DE LA INFORMATICA Y EL DERECHO

CON LA PARTICIPACIÓN DE REPRESENTANTES IBEROAMERICANOS ASISTENTES AL CONGRESO 1391

CONFERENCIA DE CLAUSURA 1425
«Tecnología de la información. Su impacto social y efectos legislativos. Algunos consideraciones» 1427

INDICE ALFABETICO DE PARTICIPANTES 1433

RELACION ALFABETICA DE PARTICIPANTES 1467

ESTADISTICAS GENERALES 1471

IV CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO 1481

PROLOGO

Supone para mí un gran honor prologar las Actas del III CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO, surgido como una necesidad de intercambio de experiencias a nivel iberoamericano, y como una decisión de actualización por parte de los profesionales de este área.

En 1989, en la ciudad de Guatemala, Sede del anterior Congreso, se anunció que la 3ª Edición tendría como Sede la Ciudad de Mérida, en España, entre otras razones, por conmemorarse en este año, 1992, el V Centenario del Encuentro entre dos Mundos, poniéndose el Congreso en fechas próximas al señalado día 12 de Octubre, en el que un descubridor llamado Cristóbal Colón pisó suelo americano, iniciándose, según los datos históricos, el Descubrimiento del Nuevo Mundo.

Otra razón de peso, a la hora de nominar a Mérida como sede de este Congreso, fue la tradición del Centro Regional de Extremadura de la Universidad a Distancia en la celebración de actos académicos relacionados con la informática y el derecho, como son los XVIII Cursos de Informática y Derecho celebrados hasta el momento, y la periodicidad de la publicación «Informática y Derecho».

En esta edición, el Congreso ha contado con la innovación, –en relación con los dos celebrados anteriormente– de que no ha habido participación de Ponentes Invitados, sino que, por primera vez, el Congreso ha versado sobre cuatro Temas Generales, expuestos en el Avance de Programa, de los que se han presentado comunicaciones, siendo la mecánica del Congreso la defensa, en sucesivas mesas, de las Comunicaciones seleccionadas.

Los cuatro grandes bloques temáticos de los que ha versado, se pueden definir en virtud de su vanguardismo y candente actualidad, como lo es el hecho de que en el mismo día en el que se analizaba en la Sede del Congreso el Proyecto de Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), éste mismo estaba siendo analizado para su aprobación en otro marco diferente, cual es el Senado español.

Se analizaron las experiencias más significativas respecto al uso de ordenadores en las actividades ejecutivas, legislativas y judiciales de las Administraciones Públicas de los países iberoamericanos, al tiempo que su utilización en el campo profesional y en la enseñanza, con la mención especial de la llamada Inteligencia Artificial (Sistemas Expertos) aplicada al Derecho, al que, dentro de los talleres, se dedicó un espacio concreto.

Por otro lado, y en el campo del Derecho de la Informática y las Telecomunicaciones, se abordaron temas tales como la Regulación Jurídica de la Informática, la Informática y las Libertades (de gran impacto social, cultural y profesional), contratos informáticos, Flujo Internacional de Datos, Delitos Informáticos, Valor Probatorio de los Soportes Modernos de Información, Transferencia electrónica de Fondos, Régimen Jurídico de la Teleinformática, Protección Jurídica de los Programas de Ordenador, etc.

Estos temas fueron expuestos, y posteriormente debatidos en los coloquios que tuvieron lugar tras las mesas de exposición, creándose así una interacción entre los asistentes al Congreso y los comunicantes, enriqueciéndose las Sesiones, con una participación pluridisciplinar.

Tras estas palabras, sobre las que intento relatar el funcionamiento del Congreso, no me queda más que agradecer a todas las Instituciones que han ofrecido su apoyo al Congreso, a todas las personas y autoridades asistentes a la inauguración, clausura, y demás actividades, y un agradecimiento a todos los congresistas, y muy especialmente a los que vinieron del otro lado del Atlántico, pues su esfuerzo ha sido mucho mayor.

Por último, felicitar a los comunicantes por su magnífica labor, y agradecer su interés en el evento.

Por nuestra parte, sólo nos queda esperar que se cumpla nuestro deseo de que de este Congreso se hayan desprendido además de unos resultados fructíferos para el avance de nuestros pueblos hacia el futuro anunciado de las Nuevas Tecnologías y Libertades, una consolidación de los vínculos entre nuestros pueblos y personas.

A todos, nuevamente gracias en nombre del Centro Regional de Extremadura de la Universidad a Distancia sobre el que recayó el peso de la organización y desarrollo del Congreso.

VALENTÍN CARRASCOSA LÓPEZ
Presidente del Comité Científico y Organizador

PRESENTACION

III CONGRESO IBEROAMERICANO
DE
INFORMATICA Y DERECHO

21 a 25 de Septiembre de 1992
Mérida (España)

PRESIDENCIA DE HONOR

Su Alteza Real

La Infanta Dña. Cristina de Borbón y Grecia

PRESIDENTE

Excmo. Sr. D. Federico Mayor Zaragoza
Director General de la UNESCO

COMITE DE HONOR

EXCMO. SR. PRESIDENTE DEL GOBIERNO
D. Felipe González Márquez

EXCMO. SR. PRESIDENTE DEL CONGRESO DE LOS DIPUTADOS
D. Félix Pons Irazazábal

EXCMO. SR. PRESIDENTE DEL SENADO
D. Juan José Laborda Martín

EXCMO. SR. PRESIDENTE DEL TRIBUNAL CONSTITUCIONAL
D. Francisco Tomás y Valiente

EXCMO. SR. PRESIDENTE DEL TRIBUNAL SUPREMO Y DEL CONSEJO GENERAL DEL PODER JUDICIAL
D. Pascual Sala Sánchez

EXCMO. SR. PRESIDENTE DE LA JUNTA DE EXTREMADURA
D. Juan Carlos Rodríguez Ibarra

EXCMO. SR. MINISTRO DE ASUNTOS EXTERIORES
D. Javier Solana Madariaga

EXCMO. SR. MINISTRO DE JUSTICIA
D. Tomás de la Cuadra Salcedo

EXMO. SR. MINISTRO DE EDUCACION Y CIENCIA
D. Alfredo Pérez Rubalcaba

EXCMO. SR. D. Francisco Fernández Ordóñez

EXCMO. SR. EMBAJADOR DE ARGENTINA EN ESPAÑA
D. Juan Pablo Lohle

EXCMO. SR. EMBAJADOR DE CHILE EN ESPAÑA
D. Juan Gabriel Valdés Soublette

EXCMO. SR. EMBAJADOR DE COSTA RICA EN ESPAÑA
D. Ignacio López Escarré

EXCMO. SR. EMBAJADOR DE HONDURAS EN ESPAÑA
D. René Arturo Bendaña Valenzuela

EXCMO. SR. EMBAJADOR DE MEXICO EN ESPAÑA
D. Jesús Silva-Herzog Flores

EXCMO. SR. EMBAJADOR DE PORTUGAL EN ESPAÑA
D. Carlos Alberto Soares Simoes Coelho

EXCMO. SR. EMBAJADOR DE LA REPUBLICA DOMINICANA EN ESPAÑA
D. Rafael Gautreau

EXCMO. SR. PRESIDENTE DE LA ASAMBLEA DE EXTREMADURA
D. Antonio Vázquez López

EXCMO. SR. DELEGADO DEL GOBIERNO EN EXTREMADURA
D. Angel Olivares Ramírez

ILMO. SR. ALCALDE PRESIDENTE DEL EXCMO. AYUNTAMIENTO DE MERIDA
D. Antonio Vélez Sánchez

EXCMO. SR. FISCAL GENERAL DEL ESTADO
D. Eligio Hernández Gutiérrez

EXCMO. SR. SECRETARIO DE ESTADO PARA LA COOPERACION INTERNACIONAL Y PARA IBEROAMERICA
D. Inocencio Félix Arias Llamas

EXCMO. SR. PRESIDENTE DE LA COMISION NACIONAL QUINTO CENTENARIO
D. Luis Yáñez Barnuevo García

EXCMO. SR. VICEPRESIDENTE DE LA JUNTA DE EXTREMADURA
D. Antonio Ventura Díaz Díaz

EXCMO. SR. PRESIDENTE DEL TRIBUNAL SUPERIOR DE JUSTICIA DE EXTREMADURA
D. Jesús González Jubete

EXCMO. SR. FISCAL JEFE DEL TRIBUNAL SUPERIOR DE JUSTICIA DE EXTREMADURA
D. Jorge Sena Argüelles

EXCMO. Y MGFCO. SR. RECTOR DE LA UNIVERSIDAD NACIONAL DE EDUCACION A DISTANCIA
D. Mariano Artés Gómez

ILMO. SR. PRESIDENTE DE LA EXCMA. DIPUTACION PROVINCIAL DE BADAJOZ
D. Ramón Rocha Maqueda

ILMO. SR. PRESIDENTE DE LA EXCMA. DIPUTACION PROVINCIAL DE CACERES
D. Manuel Veiga López

EXCMO. SR. PRESIDENTE DEL CONSEJO GENERAL DE LA ABOGACIA
D. Antonio Pedrol Rius

PRESIDENTE DEL ILUSTRE COLEGIO NACIONAL DE SECRETARIOS JUDICIALES
D. Jesús Seoane Cacharrón

PRESIDENTE DEL CONSEJO GENERAL DE LOS ILUSTRES COLEGIOS DE PROCURADORES DE LOS TRIBUNALES DE ESPAÑA
D. José Granados Weil

INSTITUCIONES ORGANIZADORAS

Extremadura EnClave 92. Junta de Extremadura.
Universidad Nacional de Educación a Distancia. Facultad de Derecho
Centro Regional para la Enseñanza de la Informática. (CREI)
Centro Regional de Extremadura de la Universidad Nacional de Educación a Distancia. Mérida.

INSTITUCIONES Y EMPRESAS COPATROCINADORAS

Aranzadi
Asamblea de Extremadura
Ayuntamiento de Mérida
Banco Central Hispano
Boletín Oficial del Estado (BOE)
Caja de Ahorros de Badajoz
Canon España
Consejo General del Poder Judicial
Consejo General de los Ilustres Colegios de Procuradores de los Tribunales de España
Diario «HOY»
Diario «EXTREMADURA»
Generalitat de Cataluña
Junta de Extremadura. Consejería de Industria y Turismo
Ministerio de Asuntos Exteriores
Ministerio de Educación y Ciencia
Ministerio de Justicia
Ministerio para las Administraciones Públicas
Unión Iberoamericana de Colegios y Agrupaciones de Abogados

COMITE CIENTIFICO Y ORGANIZADOR

PRESIDENTE
D. VALENTIN CARRASCOSA LOPEZ
Director del Centro Regional de Extremadura de la Universidad a Distancia (UNED)

SECRETARIO
D. JULIO TELLEZ VALDES
Investigador Permanente. Universidad Nacional Autónoma de México

VOCALES
D. JOSE MARIA ALVAREZ CIENFUEGOS
Magistrado-Jefe del Gabinete Técnico del Tribunal Supremo

D. MIGUEL ANGEL DAVARA RODRIGUEZ
Director del Instituto de Informática Jurídica de la Universidad de Comillas, (ICADE)

D. CARLOS DE ZULUETA CEBRIAN
Vicesecretario del Consejo General de los Ilustres Colegios de Procuradores de los Tribunales de España

D. EMILIO DEL PESO NAVARRO
Asociación de Licenciados en Informática

D. GASPAR ESCALONA MARTINEZ
Decano de la Facultad de Derecho de la Universidad a Distancia (UNED)

D. JOSE LUIS FERNANDEZ MARRON
Decano de la Facultad de Ciencias de la Universidad a Distancia (UNED)

D. FERNANDO GALINDO AYUDA
Director del Seminario de Informática y Derecho de la Universidad de Zaragoza

D. MANUEL HEREDERO HIGUERAS
Subdirector de Cooperación Internacional del Ministerio de Justicia

D. FERNANDO LUIS IBAÑEZ LOPEZ-POZAS
Vicedecano de la Facultad de Derecho de la Universidad a Distancia (UNED)

D. VICENTE LOPEZ-IBOR MAYOR
Presidente del Grupo de Trabajo de Informática y Derecho de UNESA

D. MIGUEL LOPEZ-MUÑIZ GOÑI
Magistrado del Tribunal Superior de Justicia de Madrid. Presidente de ASIDE

D. LUIS MARTI MINGARRO
Secretario General del Consejo General de la Abogacía

DÑA. BEATRIZ MARTIN DEL MORAL
Directora del Boletín Oficial del Estado (BOE)

D. JORGE PAEZ MAÑA
Coordinador de Documentación Científica del Consejo Superior de Investigaciones Científicas

D. ANTONIO ENRIQUE PEREZ LUÑO
Catedrático de Filosofía del Derecho de la Universidad de Sevilla

D. SANTIAGO RIPOL CARULLA
Profesor Titular de la Facultad de Derecho Universidad Pompeu Fabra

D. HUMBERTO RUANI
Miembro de la Comisión de Informática y Derecho del Colegio Público de Abogados de Buenos Aires

D. MANUEL RUIZ CUBILES
Director del Centro Regional para la Enseñanza de la Informática (CREI)

D. RAFAEL VELAZQUEZ BAUTISTA
Director de TECNOLEGIS

D. ANTONIO VITORINO
Magistrado del Tribunal Constitucional de Portugal

REGLAMENTO PARA LA PRESENTACION DE COMUNICACIONES

I) Las comunicaciones se presentarán en las Sesiones y Mesas respectivas de acuerdo al orden establecido por el Comité Organizador, el cual fue estructurado tomando en consideración los siguientes elementos:

1.– Agrupación temática general y particular, y en su caso, por afinidad.

2.– Orden alfabético por apellido paterno del autor, y en caso de coautoría, el del primer coautor según solicitud de registro de comunicación formulado ante la Secretaría del Congreso.

II) Sólo podrán ser defendidas aquellas comunicaciones cuyo autor o autores esten presentes en el día y hora establecidos en el Programa, salvo casos excepcionales autorizados por el Comité Organizador.

III) El tiempo de exposición será de un máximo de diez minutos por comunicación, autorizandose la presentación por varias personas, en el caso de coautoría de una misma comunicación, siempre que no se rebase el límite de tiempo anteriormente señalado.

IV) Podrán presentarse varias comunicaciones realizadas por un mismo autor, siempre que no esten comprendidas en una misma Mesa. En todo caso se regirán de acuerdo a la disponibilidad de tiempo, dando preferencia a quienes no hayan presentado ninguna comunicación hasta ese momento.

V) Posterior a la presentación de comunicaciones en cada Mesa, y siempre que el tiempo lo permita, se abrirá un periodo de preguntas y respuestas entre los comunicantes y éstos con el público; en todo caso, deberá procurarse que las intervenciones sean breves y concisas a fin de propiciar una participación mayoritaria.

VI) El Comité Organizador delega, tanto en los coordinadores de Sesión como de Mesa, la estricta observancia de estas reglas.

VII) Aquellas situaciones relativas al tema no previstas en estas reglas, serán resueltas por el Comité Organizador.

ORGANOS EJECUTIVOS DEL CONGRESO

PRESIDENTE
D. Valentín Carrascosa López (España)
SECRETARIO
D. Julio Téllez Valdés (México)
PRESIDENTES DE SESIONES Y MESAS

SESION I:	D. Miguel Angel Davara Rodríguez (España) Mesa 1: D. Guillermo Orozco Pardo (España)
SESION II:	D. Antonio Enrique Pérez Luño (España) Mesa 2: D. Rafael González-Tablas Sastre (España) Mesa 3: D. Etienne Montero (Bélgica)
SESION III:	D. Emilio del Peso Navarro (España) Mesa 4: D. Victor Blanco Fornielles (México) Mesa 5: D. Juan Diego Castro Fernández (Costa Rica)
SESION IV:	D. Humberto Félix Ruani (Argentina) Mesa 6: Dña. Yarina Amoroso Fernández (Cuba) Mesa 7: D. Santiago Ripol Carulla (España)
SESION V:	D. Miguel López-Muñíz Goñi (España) Mesa 8: Dña. Concha Alvaro (España) Mesa 9: D. Francisco Eugenio Díaz (España)
SESION VI:	D. Fernando Galindo Ayuda (España) Mesa 10: D. Rafael Velázquez Bautista (España) Mesa 11: D. Jesus Sáez Comba (España)
SESION VII:	D. José María Alvarez Cienfuegos (España) Mesa 12: Dña. María Eugenia Gayo Santa Cecilia (España) Mesa 13: Dña. María Elena Campanella de Rizzi (Argentina)
SESION VIII:	Mesa 14: D. Manuel Ruíz Cubiles (España)

EXPOSITORES

Editorial Aranzadi
Boletín Oficial del Estado
COLEX– DATA
Gobierno Vasco
SEINTEX

TALLERES

BASE DE DATOS JURIDICAS: EDIBASE

PROGRAMA:

– Presentación de las bases de datos jurídicas personalizadas: definición.

– Características principales de las bases de datos: utilización.

– Interrogación de las bases de datos personalizadas: el texto libre, por índices (temáticos y KWIC), operadores lógicos, Thesaurus.

– Las aplicaciones de las bases de datos personalizadas: Jurisprudencia, legislación y doctrina.

– Ejercicio práctico: La creación de una base de datos e interrogación.

PROFESORADO:

D. Audilio Gonzáles Aguilar. (Colombia)
Abogado. Universidad Externado de Colombia. Miembro del equipo de investigación del Grupo de Informática y Derecho de la Universidad de Montpellier.

SISTEMA Y PROGRAMA A PRESENTAR: EDIBASE

VIRUS INFORMATICOS

PROGRAMA:

– Virus: una dolencia tecnológica.

– Definición de virus (Boot, Parásitos, Multiparticos, Compañeros y Polimórficos)

– Modos de infección:
  – por infección
  – por reinfección

– Medidas preventivas

– Software comercial antivirus:
  – Detectores específicos y heurísticos.
  – Suma criptográfica.
  – Hardware.

– Sesión práctica:
  – 1º Caso: VIRUS JERUSALEN: instalación del virus en memoria; diferencia de infección entre ficheros EXE y COM; mecanismos de ocultamiento.
  – 2º Caso: VIRUS STONED: arranque con diskette; infección de diskettes y disco duro; mecanismos de ocultamiento.
  – 3º Caso: VIRUS FLIP: ejemplo de virus multipartido; infección del sector Boot, ficheros EXE y partición; mecanismos de ocultamiento.

PROFESORADO

D. Victor Manuel Tavares. (PORTUGAL)
Técnico y Experto Consultor.

SISTEMAS EXPERTOS JURIDICOS

PROGRAMA:

– Presentación de la metodología de los Sistemas Expertos: Definición, la decisión jurídica, la regla de Derecho.

– La importancia de la representación de los conocimientos y el tratamiento de datos para la realización de Sistemas Expertos.

– Importancia de la participación multidisciplinaria en la realización de los Sistemas Expertos: El experto, el ingeniero del conocimiento y el informático.

– Ejercicio práctico: La presentación de un prototipo de Sistema experto.

PROFESORADO:

D. Maurice Solet. (FRANCIA)
Experto Consultante en Sistemas Expertos en París.

D. Audilio Gonzáles Aguilar. (COLOMBIA)
Traductor.

DESARROLLO DEL CONGRESO

SESION INAUGURAL

En la Sede del Congreso, Hotel «Las Lomas», se desarrolló la sesión inaugural. El acto estuvo presidido por D. Antonio Vázquez López, y D. Jaime Naranjo Gonzalo, Presidente de la Asamblea de Extremadura, y Consejero de Educación y Cultura de la Junta de Extremadura, respectivamente, a quienes acompañaban D. Antonio Vélez Sánchez, Alcalde-Presidente del Excmo. Ayuntamiento de la ciudad de Mérida; D. Valentín Carrascosa López, Presidente del Comité Científico y Organizador del Congreso; D. Gaspar Escalona Martínez, Decano de la Facultad de Derecho de la Universidad a Distancia (UNED); D. Carlos M. Pasos Novelo, Rector de la Universidad Autónoma de Mérida de Yucatán (México); D. Manuel Ruíz Cubiles, Director del Centro Regional para la Enseñanza de la Informática (CREI); D. Vicente López-Ibor Mayor, en representación de D. Federico Mayor Zaragoza, Director General de la UNESCO; D. Jorge Sena Argüelles, Fiscal Jefe del Tribunal Superior de Justicia de Extremadura; D. Antonio Vitorino, Magistrado del Tribunal Constitucional de Portugal; y Dña. Claudia Barelli, Subsecretaria de Asuntos Registrales del Ministerio de Justicia de la República Argentina.

Hicieron uso de la palabra, sucesivamente, D. Vicente López-Ibor Mayor, que procedió a la lectura del mensaje personal que D. Federico Mayor Zaragoza envió al Congreso, D. Humberto Ruani, como Miembro de la Comisión de Informática y Derecho del Colegio Público de Abogados de Buenos Aires (Argentina); Dña. Claudia Barelli, D. Valentín Carrascosa López; D. Antonio Vélez Sánchez; y D. Jaime Naranjo Gonzalo.

De las intervenciones anteriores, destacaremos el ofrecimiento hecho por el Sr. Ruani y la Sra. Barelli de que el próximo Congreso pudiera celebrarse en Argentina.

La Conferencia inaugural corrió a cargo de D. Antonio Hernández Gil.

SESIONES ORDINARIAS

En este Congreso se ha introducido la novedad de que no se ha contado con ponentes invitados, sino que se dedicaron cuatro bloques temáticos sobre los que los interesados defendieron su comunicación, quedando así abierto a todos aquellos que pudieran aportar algo al Congreso.

Todos los trabajos seleccionados, se dispusieron en Sesiones y Mesas, y se expusieron según el calendario diseñado para ello.

Los cuatro grandes bloques temáticos versaron sobre:

TEMA I: DERECHO DE LA INFORMATICA:
- Informática y Libertades.
- Protección Jurídica del Software.
- Dinero electrónico.
- Contratación, Bienes y Servicios Informáticos.
- Deontología Informática.
- Delitos Informáticos.
- Contratación Electrónica.
- Flujo Internacional de Datos.
- Impacto de la Informática en las distintas ramas del Derecho.
- Protección de Datos.

TEMA II: INFORMATICA APLICADA AL DERECHO: PRESENTE Y FUTURO:
- Bases de Datos.
- Sistemas de Ayuda a la Decisión.
- Inteligencia Artificial.
- Informática en la Labor Legislativa.
- Lingüística Computacional y Derecho.
- Consulta Inteligente.

TEMA III: INFORMATICA Y PROCESO:
- Informática en la Administración de Justicia.
- Informática y Registro.
- Proceso Informatizado.
- Prueba Informática.
- Habeas Data.
- Las Comunicaciones Informáticas.
- Documento Electrónico.
- Informática: Garante de la Tutela Judicial Efectiva.

TEMA IV: TECNOLOGIAS DE LA COMUNICACION Y DERECHO:
- Transferencia Electrónica.
- Redes Locales y Generales de Datos.
- Integración de Redes Informáticas.
- Regulación Jurídica de las Comunicaciones.
- Mercado Unico de Valores.

La última mesa estuvo dedicada al tema PANORAMA IBEROAMERICANO DE LA INFORMATICA Y EL DERECHO, y en ésta participaron algunos representantes iberoamericanos asistentes al Congreso, entre los que podemos citar:

ARGENTINA: DRA. ELENA CAMPANELLA DE RIZZI
Secretaria Letrada de Informática.
Corte Suprema de la Nación.

BOLIVIA: LIC. JUAN CARLOS MUÑOZ
Director de Informática.
Corte Suprema de Justicia

BRASIL: LIC. FABIO GUILHERME VOGEL
Jefe del Departamento Jurídico.
Secretaría de la Ciencia y Tecnología.
Presidencia de la República.

COLOMBIA: DR. MANUEL SERRANO CASTELLANOS
Abogado. Coordinador del Programa Juriscol.
Presidencia de la República.

COSTA RICA: DR. JUAN DIEGO CASTRO FERNANDEZ
Director del Instituto Costarricense de Lógica, Informática y Derecho

CUBA: LIC. YARINA AMOROSO FERNANDEZ
Buró Ejecutivo Nacional.
Unión Nacional de Juristas de Cuba.

GUATEMALA: LIC. NEFTALY ALDANA HERRERA
Abogado y Notario.

MEXICO: ING. ROBERTO MEDINA VALLEJO
Subdirector de Informática.
Procuraduría General de la República.

PANAMA: LIC. JOSE CARLOS GARCIA SANTIAGO
Subdirector de Informática.
Corte Suprema de Justicia.

PERU: DR. PEDRO PATRON BEDOYA
Presidente de la Comisión Permanente de Informática Jurídica.

PUERTO RICO: LIC. JOSE NILO DAVILA LANAUSE
Abogado. Notario.

SESION DE CLAUSURA

El Acto de Clausura estuvo presidido por D. Manuel Amigo Mateos, Consejero de Presidencia y Trabajo de la Junta de Extremadura; D. Rafael Fernández Montalvo, Vocal del Consejo General del Poder Judicial; D. Gaspar Escalona Martínez, Decano de la Facultad de Derecho de la Universidad a Distancia (UNED); D. Jorge Sena Argüelles, Fiscal Jefe del Tribunal Superior de Justicia de Extremadura; D. Valentín Carrascosa López, Presidente del Comité Científico y Organizador del Congreso; D. Emiliano Jiménez Aparicio, Segundo Teniente de Alcalde de la Ciudad de Mérida; D. Carlos M. Pasos Novelo, Rector de la Universidad Autónoma de Mérida de Yucatán,

(México); D. José Granados Weil, Presidente del Consejo General de los Ilustres Colegios de Procuradores de los Tribunales de España; Dña. Claudia Barelli, Subsecretaria de Asuntos Registrales del Ministerio de Justicia de la República Argentina; D. Manuel Ruíz Cubiles, Director del Centro Regional para la Enseñanza de la Informática (CREI); y D. Juan Diego Castro Fernández, Director del Instituto Costarricense de Lógica, Informática y Derecho.

La conferencia de Clausura estuvo a cargo de D. Wolfrang Lohner, Director de División del Programa General de Información de la UNESCO.

Una vez finalizada la conferencia tomaron uso de la palabra, por este orden: D. Manuel Ruíz Cubiles; D. Juan Diego Castro Fernández; Dña. Claudia Barelli; D. Valentín Carrascosa López; D. Rafael Fernández Montalvo; y D. Manuel Amigo Mateos.

EXPOSICION

Durante los días del congreso, y en una Sala contigua, se realizaron exposiciones de material jurídico e informático, al tiempo que demostraciones prácticas del material informático exhibido, estableciéndose así las posibilidades y aplicaciones de estos programas destinados a profesionales del Derecho.

Estas exposiciones corrieron a cargo de empresas profesionales en el ámbito de la Informática y en el Derecho, y estuvieron coordinadas por Dña. Aurelia Trinidad Nuñez.

TALLERES

El Miércoles, día 23, en el meridiano del Congreso, se celebraron tres talleres que versaron cada uno de ellos sobre:

- Bases de Datos Jurídicos
- Sistemas Expertos
- Virus informáticos.

Estos Talleres corrieron a cargo de especialistas, y estuvieron coordinados por D. Tomás Ramírez Picarzo.

ACTOS SOCIALES

Paralelamente a las actividades propiamente técnicas y científicas del Congreso, se organizaron un conjunto de actividades, promovidas y ofrecidas por ciertas instituciones que invitaron a los Congresistas, y otras actividades turísticas.

Entre estas actividades, cabe destacar la cena ofrecida por la Asamblea de Extremadura, el cóctel ofrecido en el Parador Nacional «Vía de la Plata» por la Unión Iberoamericana de Colegios y Agrupaciones de Abogados, el Concierto celebrado en la Iglesia Santa Eulalia, ofrecido por la Coral «Au-

gusta Emérita», y la cena de Clausura otorgada por el Consejo General de los Ilustres Colegios de Procuradores de los Tribunales de España.

Paralelamente a estas actividades sociales, se programaron algunas actividades turísticas, entre las cuales merece especial atención un recorrido por Mérida, en el cual los acompañantes de los asistentes al Congreso, y éstos mismos, tuvieron la ocasión de conocer la antigua Capital de la Lusitania, y actual capital de la Comunidad Autónoma Extremeña, de la mano de un guía, que les mostró y explicó cada uno de los restos arquitectónicos de las diferentes culturas que han pasado por esta ciudad, y el Museo Nacional de Arte Romano, edificio de reciente construcción por el arquitecto Rafael Moneo, en el que están expuestas las joyas arqueológicas del Imperio Romano a su paso por España.

También se realizó un viaje a la Exposición Universal de Sevilla, EXPO'92, en el que en una agotadora jornada, se pudo contemplar el espectáculo de tan importante exposición.

En ese mismo día, y para los asistentes interesados en conocer nuestra región, se programó y realizó un recorrido turístico por Guadalupe, Trujillo y Cáceres, tres ciudades representativas de nuestra región.

PROGRAMA

LUNES 21

9,00 horas: INSCRIPCIONES

10,00 horas: INAUGURACION

10,30 horas: CONFERENCIA INAUGURAL

12,00 horas: SESION I:

MESA N.º 1

PROTECCION DE DATOS I (ASPECTOS GENERALES)

ALENDE, JORGE OSCAR
«Informática: El abuso de su poder»

BLÁZQUEZ ANDRÉS, M.ª CONSUELO y CARRASCOSA LÓPEZ, VALENTÍN
«Intimidad personal y limitaciones»

DE JULIOS CAMPUZANO, ALFONSO
«Derecho a la intimidad y publicidad de datos personales de carácter patrimonial»

DE VAL ARNAL, JOSÉ JESÚS
«La presunción de inocencia y el deber de colaboración con la inspección de trabajo. Derecho de acceder a los archivos automáticos»

FERNANDO PABLO, MARCOS MATÍAS
«Administración Pública, Informática y ciudadano: perspectiva general»

MARTÍN BERNAL, JOSÉ MANUEL y MARTÍN GARCÍA, PILAR
«Intimidad y libertades»

MONTERO, ETIÉNNE
«Las obligaciones y responsabilidades de un «titular» de fichero de datos nominativos»

ORZABAL, JOSEFINA C.
«Bases de datos, privacidad y responsabilidad civil»

SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, MANUEL
«La transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas»

SÁNCHEZ JIMÉNEZ, ENRIQUE
«Los derechos humanos de la 3.ª generación: la libertad informática»

17,00 horas: SESION II

MESA N.º 2
PROTECCION DE DATOS II (Análisis de la LORTAD)

ARROYO YANES, LUIS MIGUEL
«La cancelación de datos personales en ficheros de titularidad pública en el proyecto de LORTAD en España»

CASTILLO JIMÉNEZ, M.ª CINTA
«Estudio comparativo entre proyecto de LORTAD español y la Ley de Protección de Datos Personales de Informática portuguesa de 4/1991»

GAYO SANTA CECILIA, MARÍA EUGENIA
«Garantías del ciudadano ante la LORTAD: Posibles vías de defensa y protección de sus derechos fundamentales»

OROZCO PARDO, GUILLERMO
«Notas acerca del «Derecho de acceso» recogido en el proyecto de Ley Orgánica de regulación del tratamiento automático de datos personales»

PÉREZ LUÑO, ANTONIO E.
«Análisis crítico de la LORTAD»

RAMIRO LOZANO, INMACULADA y CARRASCOSA LÓPEZ, VALENTÍN
«La protección de datos personales en la Península Ibérica»

SANTAMARÍA IBEAS, JOSÉ JAVIER
«La LORTAD: análisis de su fundamento»

19,00 horas: SESION II (CONTINUACION)

MESA N.º 3
PROTECCION DE DATOS III (Situación Internacional)

ASPAS ASPAS, JOSÉ M.ª
«El Derecho a la Autodeterminación en la Ley Portuguesa de Protección de Datos de 1991. Sujetos, contenidos y garantías»

DE CARTOLANO, SILVIA C.
«Protección de datos personales: reforma de la constitución de Río Negro»

HEREDERO HIGUERAS, MANUEL
«La protección de los datos de carácter personal registrados con fines estadísticos en el derecho español»

MARTÍN ONCINA, JOSÉ IGNACIO
«La protección de datos informáticos en el derecho comparado»

RIPOL CARULLA, SANTIAGO
«La protección de los datos personales en el derecho comunitario»

SÁENZ GIL, RUBÉN

«Protección de datos personales sometidos a tratamiento automatizado. Normativa europea. Proyecto de ley española»

SÁNCHEZ BRAVO, ALVARO AVELINO

«El tratamiento automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: su protección»

TIRADO ROBLES, M.ª CARMEN

«La Comunidad Europea ante la Circulación de Datos Personales. Su protección jurídica»

MARTES 22

10,00 horas: SESION III

MESA N.º 4

CONTRATACION INFORMATICA Y PROTECCION DEL SOFTWARE

AMOROSO FERNÁNDEZ, YARINA

«Algunas consideraciones acerca de la protección jurídica del software»

BAUZA REILLY, MARCELO

«Protección jurídica del software en el Derecho Uruguayo»

BENITO-BUTRÓN OCHOA, JOSÉ C.

«Contrato de arrendamiento sobre bienes informáticos»

BERGEL, SALVADOR, DARÍO

«Responsabilidad Civil en materia informática»

CASTRO FERNÁNDEZ, JUAN DIEGO y CASTRO CARVAJAL, PATRICIA

«La protección legal del software en Costa Rica»

CORREA, CARLOS M.ª

«El Derecho Informático en el proyecto de acuerdo TRIPs de la rueda de Uruguay»

MIER Y CONCHA SEGURA, JORGE

«Los virus computacionales como medio de protección del software»

VAN HOUTTE, PAUL

«El seguro de la responsabilidad civil profesional de los informáticos»

12,00 horas: SESION III (CONTINUACION)

MESA N.º 5

DELITOS INFORMATICOS

ALASTULEY DOBÓN, M.ª DEL CARMEN

«Perspectiva criminológica de los delitos informáticos»

DEL PESO NAVARRO, EMILIO

«Prevención versus fraude: la auditoría informática»

GALLARDO ORTIZ, MIGUEL

«Criptología, seguridad e informática y derecho. Leyes del Ciberespacio»

GÓMEZ PERALS, MIGUEL

«Los delitos informáticos en el Derecho Español»

GUTIÉRREZ FRANCÉS, M.ª LUZ

«El borrador del nuevo Código Penal de 1992 ante la criminalidad defraudatoria por medios informáticos»

JIJENA LEIVA, RENATO

«La criminalidad informática: situación del Lege data y Lege ferenda en Chile»

TÉLLEZ VALDÉS, JULIO

«Aspectos legales de los virus informáticos»

17,00 horas: SESION IV

MESA N.º 6
REGULACION JURIDICA DE LA INFORMATICA Y LAS TELECOMUNICACIONES

DE PAZ ARIAS, JOSÉ MARÍA

«Utilización de la Informática en la Detección de comportamientos irregulares en el Mercado de Valores»

GIMENO FELIU, JOSÉ MARÍA y TENA PIAZUELO, VITELIO M.

«Régimen jurídico de las telecomunicaciones. Implicaciones comunitarias»

GONZÁLES AGUILAR, AUDILIO

«EDI (Echange Data Informatics) Intercambio de datos informáticos»

PÁEZ MAÑA, JORGE y TRIVIÑO ACUÑA, EVA

«Flujo internacional de información»

RAMOS SIMÓN, LUIS FERNANDO

«Notas sobre las nuevas tecnologías de la información y sus relaciones con el Derecho a la Comunicación»

19,00 horas: SESION IV (CONTINUACION)

MESA N.º 7
IMPACTO DE LA INFORMATICA EN EL DERECHO

BLÁZQUEZ ANDRÉS, M.ª CONSUELO y CARRASCOSA LÓPEZ, VALENTÍN

«El Derecho de la Informática en la información de juristas e informáticos»

DE NO-LOUIS y CABALLERO, EDUARDO
«El working-house informático o teletrabajo»

DURAND ALCÁNTARA, CARLOS y RIVERA SALGADO, DANIEL V.
«Derecho consuetudinario indígena e informática»

GALINDO AYUDA, FERNANDO
«Informática y derecho como asignatura para informáticos»

GONZÁLEZ TABLAS SASTRE, RAFAEL
«Aplicaciones informáticas en la enseñanza del derecho»

LÓPEZ-IBOR MAYOR, VICENTE y GARCÍA DELGADO, SONSOLES
«Situación del derecho informático en Espsña y en Europa: algunas consideraciones»

SERRADILLA SANTOS, M.ª PAZ; TRINIDAD NÚÑEZ, AURELIA y VELÁZQUEZ RODRÍGUEZ, TERESA
«Implicaciones de la informática en el ámbito laboral»

MIERCOLES 21

– VISITA A LA EXPO'92
– TURISMO REGIONAL
– TALLERES

JUEVES 24

10,00 HORAS: SESION V:

MESA N.º 8
BASES DE DATOS JURIDICAS

CASTRO FERNÁNDEZ, JUAN DIEGO
«Bases de datos constitucionales»

CORDERO ALVARADO, JUVENTINO
«Bases de datos. Elementos indispensables para la libertad profesional. Un caso de México»

DE CARTOLANO, SILVIA C.
«Banco de datos jurídicos»

DÍAZ DEL BARCO, HORACIO
«La base de datos IBERLEX del Boletín Oficial del Estado en CD-ROM»

LÓPEZ-IBOR MAYOR, VICENTE y GARCÍA DELGADO, SONSOLES
«La industria de las bases de datos y su aplicación al derecho: experiencias de la producción y distribución en el sector eléctrico»

LÓPEZ-MUÑIZ DE MENDIZÁBAL, BLANCA y VÁZQUEZ DOCAMPO, RAMÓN
«MAP LEXTER: Sistemas de bases de datos jurídicas integradas sobre administraciones territoriales»

MAZET, GUY y ORLANDO, MÓNICA
«La condición de originalidad en los bancos de datos»

RICO BONILLA, INMACULADA
«Bases de datos de legislación del Banco de España: impacto de la informática en el lenguaje jurídico»

SUÁREZ MARTÍNEZ, DIEGO F. y ALENDE, JORGE OSCAR
«Sistema argentino de informática jurídica: estado actual y evolución futura»

12,00 horas: SESION V (CONTINUACION):

MESA N.º 9
HIPERTEXTO E INFORMATICA LEGISLATIVA

AMOROSO FERNÁNDEZ, YARINA
«Legislar asistido por computadoras»

AMOROSO FERNÁNDEZ, YARINA
«Proyecto MENJUR: una alternativa válida para el perfeccionamiento y buena recuperación»

BAUZA REILLY, MARCELO
«La información jurídica: adecuado análisis, correcto funcionamiento y buena recuperación»

DOMÍNGUEZ LUIS, JOSÉ A.
«Informática y técnica legislativa»

GONZÁLES AGUILAR, AUDILIO
«Hipertextos y Derecho»

LIMA TORRADO, JESÚS y ROVETTA CLYVER, FERNANDO
«Hipertexto y Derecho»

RAMIREZ HUAMAN, JORGE L.
«El aspecto de la interpretación jurídica en el tema de los sistemas expertos aplicados al Derecho»

17,00 horas: SESION VI:

MESA N.º 10
INFORMATICA DECISIONAL Y SISTEMAS EXPERTOS

CAMMELLI, ANTONIO Y SOCCI, FIORENZA
«Sistemas automáticos y Derecho. Lexis: un sistema experto jurídico de ayuda a la decisión y para una mejor redacción normativa»

CORDERO ALVARADO, JUVENTINO y BERMÚDEZ GÓMEZ, SALVADOR
«Bases de conocimiento en la consulta legal»

DÁVARA, MIGUEL ANGEL
«Introducción a los sistemas expertos»

LASALA CALLEJA, PILAR; LEKUONA AMIANO, ALBERTO; LACRUZ CASAUCAU, BEATRIZ; AGUARÓN JOVEN, JUAN y PEINADO VISANZA, ROSARIO
«Generación de una bases de casos para un sistema experto que razona por analogías»

LÓPEZ-IBOR MAYOR, VICENTE y OLIVIÉ MARTÍNEZ PEÑALVER, LUIS
«Sistemas de ayuda a la decisión en el ámbito jurídico de la contratación»

LÓPEZ MUÑIZ DE MENDIZÁBAL, BLANCA
«Sistemas expertos: viabilidad de su aplicación al derecho»

MORENO, JOSÉ ANGEL
«Sistemas de ayuda a la decisión en las administraciones públicas»

PÉREZ DE LA CRUZ, JOSÉ LUIS; AURIOLES MARTÍN, ADOLFO; BELMONTE MARTÍNEZ, M.ª VICTORIA y HERNÁNDEZ PASCUAL, AMPARO
«Un sistema experto en derecho cambiario»

17,00 horas: SESION VI (CONTINUACION):

MESA N.º 11
INFORMATICA JUDICIAL

BRENNA, RAMÓN GERÓNIMO y BIELSA, RAFAEL A.
«Organización de la justicia y nuevas tecnologías»

CAMPANELLA DE RIZZI, ELENA M.
«Informática judicial documental y de gestión en el poder judicial de la nación de la República de Argentina»

CARRASCOSA LÓPEZ, VALENTÍN
«La gestión automatizada en el ámbito de la Justicia Española»

DÓVALO TABOADA, JOSÉ y ALIE COLL, ENRIQUE
«Evolución en el período 89-92, de los proyectos de informatización de la Administración de Justicia expuestos en el I Y II Congresos Iberoamericanos de Informática y Derecho»

ELORZA URBINA, MIKEL
«Propuesta de modernización de la Administración de Justicia. Plan de informatización de la Administración de Justicia en Euskadi»

GARCERÁN CORTIJO, ANTONIO
«Las comunicaciones informáticas: Colegio de Procuradores-Administración de Justicia»

GONZÁLEZ RODRÍGUEZ, FRANCISCO PEDRO
«La informática en la Administración de Justicia»

GUERRA GIMENO, ANTONIO y SÁNCHEZ GUIU, IÑAKI
«Informatización de la Administración de Justicia en Euskadi. Una experiencia concreta: la gestión del orden jurisdiccional civil»

HURTADO, CARLOS FELIPE
«Nuevas tecnologías en el proceso y en el servicio de la Administración de Justicia»

MUNICIO SANZ, GREGORIO
«La informática y el procedimiento administrativo de apremio»

OTEROS FERNÁNDEZ, MANUEL
«El Secretario judicial y la informatización integral de los Juzgados de primera instancia»

VIERNES 25

10,00 horas: SESION VII:

MESA N.º 12
INFORMATICA JURIDICA Y REGISTRAL

ALIE COLL, ENRIQUE y DÓVALO TABOADA, JOSÉ
«Integración de la gestión informática judicial en el área Iberoamericana»

AMENTA, PAULO MARCO y FERNÁNDEZ, RUBÉN IGNACIO
«Informatización de solicitudes mineras en la provincia de Tucuman»

ARENA, ALICIA; BIELSA, RAFAEL; VILAS, JORGE y GUTIÉRREZ, ANÍBAL
«Metodología para la reconversión de un sistema público automatizado de información jurídica»

BUENO MALUENDA, M.ª CRISTINA
«La nueva gestión tributaria local: IBI Y Catastro»

COLLADO, JUAN CARLOS
«Automatización del piso de remates en la bolsa mexicana de valores»

COMISIÓN DEL COLEGIO PÚBLICO DE ABOGADOS DE ARGENTINA
«La informática aplicada al derecho: presente y futuro»

DE CARTOLANO, SILVIA C.
«Proyecto de informatización del registro de la propiedad inmueble de la provincia de Neuquem»

JOVER I PADRO, JOSEP
«El proyecto de colegios de Abogados de Barcelona en el ámbito de la informática jurídica»

OROS Y MURUZÁBAL, MIQUEL
«La informatización de la medicina forense en Cataluña. Ventajas conseguidas tras cinco años de implantación»

RAMÍREZ HUAMAN, JORGE L.

«Informática y Administración de Justicia en el Perú: apuntes a propósito de un proyecto»

RUANI, HUMBERTO FÉLIX

«Función integradora de la informática jurídica en las ramas del Derecho Iberoamericano: aporte de la Ley a la transferencia electrónica de fondos en la Corte de Casación Penal y el Sistema Argentino de Informática Jurídica»

12,00 horas: SESION VII (CONTINUACION):

MESA N.º 13
PROCESO INFORMATIZADO Y DERECHO DE PRUEBA

ALVÁREZ-CIENFUEGOS SUÁREZ, JOSÉ MARÍA

«Las obligaciones concertadas por medios informáticos y la documentación electrónica de los actos jurídicos»

BAUZA REILLY, MARCELO

«Apertura del Derecho probatorio uruguayo en materia de nuevas tecnologías de información»

CASTRO FERNÁNDEZ, JUAN DIEGO y GARRO CANESSA, JAIME

«El habeas data en Costa Rica»

COSENTINO, GUILLERMO R.

«Informática y Proceso»

DE ZULUETA CEBRIÁN, CARLOS

«El procurador en el Proceso Informatizado»

FERREYROS SOTO, CARLOS

«Automatización de la instrucción penal ordinaria en el Perú: análisis y proposiciones»

LLACER RUBIO, ENRIQUE; LUNA HUERTAS, PAULA y RUIZ DEL CASTILLO, JOSÉ CARLOS

«Ultimas tecnologías en soportes electrónicos y su utilidad para los profesionales del derecho»

LÓPEZ-MUÑIZ GOÑI, MIGUEL

«El proceso informático Multimedia»

VAQUERO CARBALLO, JESÚS

«La informática en los centros penitenciarios»

17,00 horas: SESION VIII:

MESA N.º 14
PANORAMA IBEROAMERICANO DE LA INFORMATICA
Y EL DERECHO

CON LA PARTICIPACION DE REPRESENTANTES IBEROAMERICANOS ASISTENTES AL CONGRESO

20,00 horas: CLAUSURA OFICIAL
ENTREGA DE DIPLOMAS

Mensaje del Director General de la UNESCO

D. FEDERICO MAYOR ZARAGOZA

Constituye para la UNESCO un honor y especial motivo de satisfacción desempeñar la Presidencia de este III Congreso Iberoamericano de Informática y Derecho. Compromisos previos de imposible cancelación me impiden hoy, como sería mi deseo, acompañarles personalmente en este acto de solemne apertura del mismo. Pero quiero, sin embargo, hacerles llegar este mensaje de sincera felicitación por el acierto y la oportunidad de esta convocatoria, y de estímulo para la eficaz orientación de sus análisis y la puesta en práctica de sus resultados.

Celebro asímismo que la sede de este III Congreso sea la bella ciudad extremeña de Mérida, de modo particular cuando conmemoramos el V Centenario del Encuentro entre dos Mundos. El año 1492 representa el inicio de un proceso de conocimiento y reconocimiento recíproco entre todos los pueblos de la Tierra, cuya culminación aparece hoy más necesaria y perentoria que nunca.

Desde aquel momento la historia fragmentada de la Humanidad sería universal, la condición humana única, más allá de las diferencias existentes entre culturas y civilizaciones. El hilo conductor de las lenguas ibéricas permitió no sólo la liberación y la independencia sino que puso de relieve el valor y diversidad de las lenguas vernáculas. Desde Nebrija hasta Bolívar, desde Vasconcelos a Paz, UNAMUNO, BORGES, o SÁBATO la aproximación de los dos mundos encuentra en el patrimonio cultural lengua compartida y en el ansia de conocimientos sus referencias principales.

Desafiando al tiempo y al espacio, la historia de la humanidad viene observando en los últimos decenios un nuevo encuentro de singulares características: un mayor acceso de la condición humana a su propia «memoria colectiva» y, sobre todo, la posibilidad de una mayor participación, especialmente a escala municipal. «Participo, luego existo», es la traducción de la sentencia cartesiana en términos de auténtica ciudadanía.

A velocidades vertiginosas este «encuentro» alcanza las distintas ramas del saber, invade todas las actividades profesionales y la propia esfera individual de nuestras vidas. En efecto, el fabuloso progreso de los medios tecnológicos de la información y de la comunicación impulsa la transformación radical de los derroteros y horizontes de las sociedades contemporáneas, y constituye un reto a la composición de sus modelos de autoridad y organización. Sus esquemas institucionales y estrategias de acción deben adaptarse sin demora. El

propio comportamiento se ve afectado seriamente. Parece claro que si se superan los riesgos de uniformización y alienación, sólo con los nuevos resortes que la ciencia y la tecnología ponen a nuestro alcance se podrá hacer frente a la globalidad y a la complejidad progresiva de los desafíos presentes.

ANTHONY SMITH, en su conocida obra Goodbye Gutenberg, señala que la revolución de la información nos ofrece un paso hacia un nuevo tipo de Alejandría, es decir, hacia una abundancia de información, universalmente asequible, pero en la que las restricciones surgen en sus modos de depósito y de clasificación, más que de los impedimentos más tradicionales que fueron la censura y el control gubernamental. Se trata de un sistema electrónico que permite compartir, comparar y aumentar la totalidad del conocimiento.

Sin embargo, esta concentración del saber conseguida a través de las nuevas tecnologías informativas, puede facilitar también una utilización abusiva de la información acumulada. La consigna utilitarista de SIR FRANCIS BACON «saber es poder», convertida ahora en «información es poder» no conlleva una renuncia incondicional al sistema de garantías del Estado de Derecho, en aras de poner el conocimiento al servicio exclusivo de la utilidad técnica y económica, sino que, al contrario, nos debe invitar a su fortalecimiento.

Ya en 1968, la Asamblea General de las Naciones Unidas reconoció la importancia de la información atribuyéndole un papel confluyente entre la ciencia y la tecnología y pidió que su análisis fuera objeto de un estudio global. En 1974 decidió que el Comité de Ciencia y Tecnología para el Desarrollo actuara como centro de convergencia de las actividades relacionadas con la aplicación de la ciencia y la tecnología de las computadoras para el desarrollo de todos los países, en especial de los países en vía de desarrollo, teniendo en cuenta sus problemas concretos y que, para ayudarles en esta tarea, utilizara principalmente los servicios de expertos, tanto de las Naciones Unidas (como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y el Comité Asesor sobre la Aplicación de la Ciencia y la Tecnología al Desarrollo) u otras organizaciones intergubernamentales competentes como la Oficina Intergubernamental de Informática.

Desde entonces numerosas han sido las acciones y programas que se vienen sucediendo a fin de tratar de dar en cada caso las respuestas y sugerencias más pertinentes a un problema global, el informático, cuya imbricación con otros saberes y, por tanto, su interdisciplinariedad, es razón misma de desarrollo.

El Derecho, «Ars Longissima», se identifica con la sociedad y con su historia. Si es misión primera del Derecho normar, regular, ordenar la vida, las vías de comunicación entre experiencia y solución jurídica, deben ser fluídas y acordes con el contexto temporal en que se actúa.

Es por ello especialmente necesario que la Ciencia del Derecho, la administración de la Justicia y los hombres que la sirven, adapten sus destrezas y métodos de trabajo a la nueva realidad tecnológica de nuestro tiempo.

Considero por todo ello ejemplar la labor emprendida por las instituciones convocantes de este III Congreso Iberoamericano de Informática y Derecho. Después de aquella «trabajosa primera piedra artesana» que supuso la primera reunión de Santo Domingo, llega ahora el momento de abordar «in extenso» el amplio marco de relaciones que cubre este feliz maridaje de la Informática y el Derecho. Nuevas tecnologías y libertades es el acertado frontispicio elegido para orientar sus reflexiones.

Disponemos de inmensos recursos tecnológicos, pero debemos afianzarlos sobre principios y valores intransitorios. Tenemos todavía los pies de barro, acosados por miopes intereses e incapaces de realizar las transformaciones de la profundidad y celeridad debidas. Llegamos a considerar irremediable lo que sólo es intolerable como los patéticos acontecimientos de Somalia, que son una afrenta a la dignidad humana en su conjunto.

La defensa de las libertades es hoy, si cabe, más exigente, más necesaria, más insustituible. Defensa contra toda sombra de límite o de sesgo, cualquiera que sea el procedimiento o medio –tecnológico o no– utilizado.

La actualidad, pues, del Congreso es indudable. Actualidad en el sentido castellano del vocablo: tiempo presente y también en el latino que ha pasado a las lenguas sajonas: realidad. Evaluar la realidad jurídica con la mirada atenta a la evolución tecnológica alcanzada. Evaluar la asociación de la tecnología y las libertades a la altura de nuestro tiempo.

Poner ambos conceptos en relación es ya una exigencia y un incentivo intelectual, es decir, ético, de primer orden, del que la UNESCO no podía, ni quería, estar ausente.

Conferencia Inaugural

D. ANTONIO HERNANDEZ GIL

Presidente de la Real Academia de Jurisprudencia y Legislación
Ex-presidente del Tribunal Supremo y del Consejo General del Poder Judicial
Ex-presidente del Congreso de los Diputados
Ex-presidente de la Real Academia de Extremadura de las Letras y las Artes

Ante todo agradezco que se me haya dado la ocasión de intervenir en esta expresión de la realidad iberoamericana que es el presente Congreso sobre un tema tan atractivo e intercomunicante como la informática y el derecho. Muchas gracias también al Dr. VALENTÍN CARRASCOSA por las cariñosas palabras que me ha dedicado.

I
PLANTEAMIENTO GENERAL

Desde hace ya bastantes años, la informática no sólo ha invadido, y transformado la vida cotidiana. También ha revolucionado el discurso científico general y, sobre todo, su aplicación en disciplinas concretas: la física, la astronomía, la biología, por poner algunos ejemplos obvios, no serían hoy las mismas sin el poder de cálculo de los ordenadores. Cuando se trata de números o magnitudes no cabe dudar del papel sustancial de la herramienta informática. El Derecho, sin perjuicio de algunos aspectos cuantitativos, es, por esencia, el dominio de lo cualitativo, del contenido, del matiz, frente a lo que sólo puede ser verdadero o lo falso, expresiones paradigmáticas de esa lógica binaria que está en la base del lenguaje informático.

Sin embargo, la Informática y el Derecho en estos años han ido afianzando su capacidad de unión e interacción.

Algunos autores, como FROSINI, subrayan que el encuentro tiene algo de «sorprendente» porque el Derecho es la más antigua forma de la cultura humana, que ha permanecido ajeno al mundo de la ciencia experimental y aplicada hasta el punto que sólo se ha servido durante mucho tiempo de la pluma de escribir, mientras la informática es exponente de la tecnología más avanzada en la civilización contemporánea. Viendo así las cosas, podría pensarse incluso

casi en un rechazo. Pero esta es una visión del problema algo superficial y anecdótica. Aunque la pluma y la imprenta hayan sido los únicos instrumentos mecánicos utilizados para exteriorzar el Derecho, dentro, en el contenido ordenador del Derecho y en el tratamiento técnico y científico del mismo, siempre ha habido un proceso de racionalización. Y esto hay que tenerlo en cuenta desde el punto de vista de la informática, que es mucho más que una mecánica sofisticada.

Por otro lado, en la confluencia de la informática y el Derecho, también es preciso ponderar cómo éste, por la creciente multiplicación y complejidad con que se viene manifestando, demanda nuevas formas de tratamiento y de conocimiento. La informática no es simplemente recibida; es bien recibida y, más aún, es exigida.

II
EL USO DE LA INFORMATICA EN LA VIDA DEL DERECHO

Hay un aspecto práctico en el que la presencia de la informática es cada vez más patente. Desde el nivel más elemental del uso personal de la informática por el jurista en el desenvolvimiento regular de su quehacer redactando escritos, almacenando y ordenando datos, consultando jurisprudencia o legislación desde su terminal de ordenador. Hasta el nivel más complejo de las grandes redes informáticas al servicio de la Administración de Justicia, organizando la gestión de la oficina judicial, interconectando Juzgados y Tribunales para agilizar, hasta hacerla instantánea, la comunicación entre ellos o entre ellos y otros órganos de la Administración Pública.

Lo que explica este uso masivo y creciente de la informática en el derecho son dos datos básicos: la creciente necesidad de procesar cada vez más información y la creciente necesidad de intercambiar esa información, de comunicarse.

1.– La frondosidad legislativa.

La proliferación legislativa ha dejado de ser una fuente de metáforas más o menos afortunadas (como la que habla hoy de la legislación motorizada) para ser sólo una realidad inabarcable en la que no sólo ha crecido la cantidad de las normas. Ha crecido también la complejidad de las relaciones internas entre las normas, haciendo, por ejemplo, enormemente difícil la determinación de las derogaciones tácitas derivadas de un cambio legislativo. Como han crecido las fuentes del Derecho y los destinatarios de las normas. De modo parecido a lo que sucedía en la larga época del Derecho común, basada en el predominio del derecho romano frente a toda suerte de Derechos locales, primero y nacionales, después, hoy nos encontramos también con un espacio normativo pluridimensional en el que coexisten normas locales, autonómicas, generales, comunitarias o internacionales. Si es difícil acceder al dato normativo, o identificarlo, más difícil todavía es determinar su validez, y tener en cuenta eso que SAVIGNY conceptuaba como el elemento sistemático de la interpretación normativa, y el

Título Preliminar de nuestro Código Civil, en su art. 3.1, denomina el contexto de la norma. Definir la norma en su contexto total, única forma de poder interpretarla, es harto problemático.

Pero en el Derecho, en última instancia, parece no haber mucho espacio para la novedad. Alguna vez hemos dicho, y aquí en Mérida la apreciación puede tener un significado especial, que si un ciudadano romano reviviera entre nosotros, una de las pocas materias de las que mejor podríamos hablar con él sería de Derecho.

La situación normativa que hemos intentado describir se parece bastante a la que existía antes de la Codificación. Los Códigos civiles fueron un remedio contra la dispersión normativa y la incertidumbre jurídica, aún a costa, para los detractores de la Codificación, de sacrificar la riqueza de los contenidos y la agilidad de la adaptación y la innovación. De forma semejante, los Tribunales Supremos se crearon en los países europeos para unificar y hacer abordable y utilizable la jurisprudencia. Hoy la propia jurisprudencia del Tribunal Supremo necesita ser reunida, ordenada y procesada para ser utilizable.

Como ya dije en la primera ocasión que me ocupé de la informática jurídica, existe un paralelismo histórico e ideológico entre ella y la empresa codificadora. Hace aproximadamente dos siglos, la Codificación, propugnada inicialmente por el racionalismo de la Ilustracion para tomar inmediato contacto con el entendimiento de la ley como manifestación de la voluntad general, que fue uno de los primeros pasos de la democracia, alentó el ideal y el propósito de lograr una enunciación clara, correcta, completa y definitiva del ordenamiento jurídico que había de quedar sistemáticamente condensado en unos cuantos libros, los códigos, los mismos dentro de cada Estado, en contraste con las normatividades del viejo arrastre y diverso origen, unas veces locales, con residuos estamentales y estatutarios, y otras, por el contrario, de generalidad superior a la de la propia demarcación estatal, según ponen de relieve creaciones entre sí tan distintas como son el sistema del Derecho Natural y el fenómeno de la recepción del Derecho Romano. El ordenamiento jurídico, que carecía de unidad de sentido, era difícilmente identificable.

En algún aspecto, la informática viene a ser, dos siglos después de la Codificación, la reencarnación y el replanteamiento de las mismas ante los problemas de hoy, de acuerdo con los avances tecnológicos de nuestro tiempo.

En cierto modo, la informática jurídica acude en auxilio o en sustitución de los Códigos que, siendo poderosos, advinieron impotentes para realizar su intento. Un día y durante algún tiempo compendiaron el Derecho. Todavía subsisten muy llenos de retoques; pero están ampliamente desbordados por una corriente circulatoria que de un modo incesante y creciente genera normatividades numerosas y complejas.

El paralelismo entre la Codificación y la informática jurídica se manifiesta igualmente en la contradicción crítica a que una y otra han dado lugar. Lo

mismo que el romanticismo de la escuela histórica, invocando el espíritu del pueblo, la tradición y las singularidades de la cultura, se oponía a un Derecho racionalizado y homogéneo, así también ahora, desde posiciones esgrimidas como humanistas y éticas, se mira con reparos la intromisión de la máquina, en la que quiere verse una competidora del hombre. Tal actitud es fruto de un conservadurismo digno, claro es, de respeto a condición de que no reivindique para sí la única actitud humanista. Pero sería curioso, anacrónico y contradictorio que los profesionales del Derecho hubiéramos de cumplir nuestra misión encerrados en el pequeño reducto de un taller personal y artesano. Detenerse en la electricidad sin servirse de la electrónica equivaldría a haberse detenido en la escritura sin utilizar la imprenta. Ninguna posición regresiva está llamada a imponerse. Termina siempre por imponerse el progreso, generalmente más allá de las formas preconizadas por la fuerza revolucionaria de la imaginación creadora.

Salvando, pues, las distancias, la informática hoy puede jugar un papel semejante al de la Codificación en la búsqueda de la certidumbre jurídica. De momento, desde fuera de la producción del dato normativo o jurisprudencial, ordenando su presentación, facilitando su acceso y, quizás, suministrando las conexiones necesarias para tener la certeza de su existencia o validez. El día de mañana, acaso la propia generación de las normas, o de los conjuntos normativos, o incluso la de las sentencias –y no nos referimos a un aspecto valorativo, de búsqueda de la decisión justa– no pueda desligarse del soporte y el lenguaje informático.

2.– La informática en la comunicación.

El soporte electrónico de la informática la orienta de suyo a la comunicación. Cabe pensar en una red total en la que todos los agentes del mundo jurídico se hallan interconectados: la presentación de escritos judiciales, las notificaciones, la consulta de resoluciones de un campo mucho más ámplio de órganos jurisdiccionales... Todo ello podría realizarse prácticamente casi al mismo tiempo.

La informática como instrumento de comunicación electrónica ofrece ya realidades o figuras jurídicas nuevas en el mundo de la contratación o, en el ámbito procesal, en el de la prueba. Si hace algunos años empezó a hacerse frecuente la pregunta por el valor de la comunicación por telefax como forma de contratación o como medio de prueba, ahora comienza a tener sentido la cuestión de la contratación informática mediante el empleo del correo electrónico de ordenador a ordenador o de los soportes magnéticos de los ordenadores como medio probatorio. La dogmática alemana habría hablado quizás, para tales supuestos, de relaciones contractuales o negociales de hecho. Sin embargo, la generalización de estos procedimientos y la importancia de la contratación a que se refieren obligan a replantearse quizás aspectos tradicionales de la teoría general del contrato como el del momento de la perfección del contrato, o conceptos como el de las declaraciones receptivas de voluntad.

Como quiera que sea, lo cierto es que el uso de la informática en la vida del Derecho no representa sólo un instrumento útil. Gradualmente, como suele suceder, va produciendo cambios cualitativos en la manera de tratar con la materia jurídica. Tal vez un ejemplo, todavía menor, que ilustra este cambio lo podemos ver en la forma de la Sentencia. Especialmente en algunos órdenes jurisdiccionales y materias (los juicios laborales, los ejecutivos), el discurso de la Sentencia se ha uniformado: el fallo va precedido de un encabezamiento y unos antecedentes de hecho que apenas tienen otros elementos variables que los datos de las partes y los de la pretensión, y unos fundamentos de Derecho que se contruyen mediante la elección y combinación de unos cuantos factores constantes. La informática consiste, a la postre, en una generalización de los modos de procesar la información y tiende, por tanto, a la uniformidad y a los procedimientos combinatorios.

La construcción de estos modelos argumentativos es posible sobre todo en materias propensas a la uniformidad, el esquematismo y la reiteración. Pese a todas estas atenuaciones, el cambio que se da en la construcción de la Sentencia –y en la concepción de la misma– es cualitativo. Parece, en principio, que todo consiste en ahorrar tiempo y escritura, ya que la redacción ex novo y puntual se sustituye por unos párrafos estandarizados que son los modelos grabados en la memoria del ordenador. Sin embargo, aunque la facilidad sea cierta y atractiva, cabe preguntarse si no se invierte el proceso de establecimiento de la Sentencia, exigiéndose en medio de construcción y argumentación lo que se concibió como simple medio de expresión. Por esmerada que sea la labor de distinción y ajuste entre la parte preconfigurada de los argumentos y la parte original, ¿no habrá cierta inclinación a lo primero? ¿quedará suficientemente atendida la carga humana e individualizadora de cada caso? Tampoco es desdeñable el sentimiento de frustración que puede producirse en las partes y en los profesionales que intervienen en su interés. Porque puede parecer como si la Sentencia, más que una refundición de la norma jurídica con los hechos, es una preponderancia de lo normativo a través de una conducta procesal ritualizada, aunque el rito esté completamente secularizado. Con todo, la masificación de la aplicación judicial del Derecho encuentra en la informática un instrumento que la dinamiza con el que es preciso contar. Extremar los cuidados y los límites es preferible a cerrar los ojos. También es esta una realidad a la que el Derecho ha de servir y de la que el Derecho debe servirse.

Pero el significado de la informática, incluso en este aspecto práctico que estamos considerando, no es sólo externo o de procedimiento. Uno de los productos más relevantes que la informática ofrece a los juristas está representado por las bases de datos o Thesaurus, sean la legislación, jurisprudencia, bibliografía o integrados. Independientemente de sus condiciones de utilización y su valor más o menos instrumental, la construcción de tales bases de datos incluyen una tarea delicada de indexación de aquellos items

o tópicos que posteriormente van a emplearse para buscar o seleccionar información o para interconectarla. Tales índices no tienen nada que ver con los índices lineales poco estructurados de los procedimientos escritos.

La complejidad de los niveles en que se organicen los tópicos, la profundidad de las estructuras arborescentes, o la cantidad de las referencias cruzadas de que pueden dar cuenta son mucho mayores. En el plano más superficial, los índices pueden coincidir con palabras, pero también pueden introducirse conceptos abstractos y redes de conceptos deducidos del lenguaje científico de los juristas con el tamiz de las exigencias lingüísticas propias de la informática. El lenguaje jurídico desvela ciertos elementos invariantes cuya combinación, potencialmente infinita, genera la diversidad de reglas de Derecho o Instituciones. El lenguaje informático puede tratar esos elementos invariantes para organizar la información jurídica y procesarla.

Seguimos estando junto a la tradición del pensamiento jurídico. En la plenitud de la dogmática jurídica, IHERING, en su obra el «Espíritu del Derecho Romano», decía que todos los verdaderos juristas de todos los países hablaban un mismo lenguaje. Atisbaba IHERING la tarea de identificar un alfabeto jurídico universal que, como el alfabeto del lenguaje natural, permitiera explicar cualquier institución por la combinación de una serie limitada de elementos simples e invariantes, como las letras del alfabeto.

La informática jurídica, aunque sólo sea para tratar y ordenar datos, obliga a traducir el lenguaje de las normas y el de los juristas a otro lenguaje en el que los contenidos jurídicamente significativos de aquéllas vienen representados por un conjunto estructurado de conceptos jurídicos capaces de dar cuenta de la multiplicidad de supuestos de las relaciones sociales.

La informática, en todas sus aplicaciones, requiere una depuración de los términos y de las expresiones más allá de cómo éstos los muestra el lenguaje natural. No se trata de que el lenguaje natural sea pobre o imperfecto y necesita ser enriquecido. La obra social, colectiva y racional, irreflexiblemente racional, que es una lengua, no puede ser realizada ni suplida por los actos individuales de la racionalización técnica. Por eso, el lenguaje natural es extraordinariamente rico y fecundo. Lo que se requiere para la operatividad informática es precisamente una esquematización, acaso un empobrecimiento semántico y sintáctico en busca de la precisión.

La reducción lingüística o léxica con vistas a la informática representa una racionalización de segundo grado: esto es, superpuesta a la que todo el lenguaje contiene por sí. Es una racionalización, a diferencia de la del lenguaje natural, reflexiva y subsiguiente o de segundo grado. Supone el acercamiento del sistema lingüístico, que está construido para un universo infinito de aplicaciones, a un sector finito y limitado de aplicación.

El uso de la lengua mediante el habla consiste en la combinación de signos que, asociándose y poniéndose, enuncian significados y formulan men-

sajes. En esto mismo hay que insistir, al preparar el lenguaje para la informática, sólo que restringiendo el universo semántico, así como las iniciativas del hablante, con el fin de lograr una mayor precisión.

La informática necesita un lenguaje objetivado, rigurosamente designativo o denotativo; la connotación, que implica la presencia de la personalidad del hablante y del contexto, deja de ser utilizable. Es claro que los ordenadores, con el automatismo que les caracteriza, no pueden emitir giros connotativos. En general, desaparecen los componentes psicológicos del discurso para ser reemplazados por la operatividad lógica. Como también desaparecen las posibilidades –y esto puede ser peligroso– de la contribución ética a la solución de los casos. La ética del enunciado normativo es, ciertamente, posible; mas resultan muy limitadas las posibilidades de su acomodación a las circunstancias: Así ocurrirá, por ejemplo, con el principio de la buena fe, que sólo traducido normativamente en determinados contenidos podrá actuar. El lenguaje informático, al objetivarse, objetiva también el propio razonamiento jurídico. A consecuencia de ello gana en seguridad, pero pierde fluidez. El trayecto discursivo requiere un trazado con una señalización perfecta y sin ambigüedades.

Por otro lado, también por su papel en la comunicación, la informática en general y en particular la jurídica traen consigo una socialización del conocimiento. La socialización nos inunda en muy diferentes versiones. Esta es quizá la de más ámplio espectro. Los ordenadores ponen a dispoción de todos un caudal informativo para obtener el cual, sin ellos, se requeriría ocupar una posición privilegiada. Por ejemplo, el hallazgo de un dato jurisprudencial preciso ya no dependerá de que el abogado disponga de una buena biblioteca y de un equipo de colaboradores. El terminal del ordenador estará dispuesto a facilitarlo a quien se acerque a él e incluso a ayudarle en la formulación de la correspondiente pregunta. Otra manifestación de la socialización es que el propio discurso jurídico pierde connotaciones éticas. Especialmente esto último puede ser peligroso, aunque también tiene sus peligros el subjetivismo ético. Hay, en suma un proceso de racionalización que tiende hacia la objetivación del discurso que por lo mismo se despersonaliza y se hace más uniforme.

La confluencia de la informática con el Derecho (o si se prefiere con el ordenamiento) obedece a un doble impulso. Por un lado nos encontramos con que la informática llega al Derecho y en él produce un impacto: el impacto que produce, como he dicho en otra ocasión, esa vanguardia de la modernidad que es la tecnología de los ordenadores. Este llegar no es un simple llegar también, como está llegando a todo, a las distintas realidades de la vida. Llega precisamente a lo que configura como un orden, como un sistema. La función sistemática de la informática ha introducido el sistema en muchos ámbitos en donde no lo había, creándolo de nueva planta. No es lo mismo en el Derecho que se caracteriza por lo que tiene de suyo de organi-

zación, de normatividad y de conformaciones y soluciones. Por tanto, penetra en un terreno que le es especialmente propicio. He aquí el otro impulso: la necesidad que el propio Derecho siente de la informática.

3.–La informática como disciplina en la reflexión científica o metodológica acerca del Derecho.

Llegando a un nivel más alto, la informática proporciona a la ciencia del Derecho un instrumento de reflexión, análisis y construcción, un lenguaje, de alto valor. En los últimos años son muchas las tesis doctorales, por ejemplo, que se han ocupado de las relaciones entre la lógica jurídica, ya sea la lógica deóntica o la lógica apofántica, la informática, los lenguajes artificiales y el análisis del lenguaje jurídico o normativo. No es sólo consecuencia de la mencionada introducción de la informática en la vida cotidiana del jurista.

Como decía WITTGENSTEIN, la lógica es por definición tautológica; es decir, sólo sabe obtener de sus proposiciones aquello que previamente se ha introducido en ella, se pliega sobre sí misma en un discurso formal que excluye la relevancia de cualquier contenido material, salvo en cuanto a las condiciones de verdad o falsedad de los enunciados que tratan de contenidos materiales (o a las condiciones de validez o invalidez si se trata de enunciados normativos). El positivismo lógico que emerge en este siglo, sobre todo, del llamado Círculo de Viena, primero, y la filosofía analítica después, propiciaron un auge de los estudios de lógica formal que no dejó de alcanzar al Derecho. En cierto modo puede decirse que es una corriente de pensamiento o metodológica que parece agotarse, quizás por su excesivo formalismo y la ausencia de contenidos o de objetivos fuera del discurso lógico en sí mismo.

De igual modo puede decirse que la informática jurídica, en su aspecto científico o metodológico, ha tomado en parte el relevo. Si la lógica es esencialmente tautológica, la informática posee, en cambio, una vocación de proyectarse fuera de sí. Presupone el formalismo del lenguaje lógico, pero lo proyecta sobre un objeto externo bajo la especie de información, siendo así que todo puede considerarse como información, desde los enunciados normativos hasta los asertos de los Jueces, o los juristas, sobre las normas o enunciados normativos.

Por otro lado, en la medida en que la informática trata de procesos de información siguiendo las pautas formales, como las reglas o la sintaxis de un lenguaje artificial, es fácil deducir un isomorfismo entre los procesos informáticos y los procesos racionales que subyacen a la actividad discursiva del jurista. Lo que en el plano operativo es la Inteligencia Artificial, expresión con la que se denota la simulación o reproducción por procedimientos informáticos del razonamiento humano «inteligente», en el plano teórico le permite a la informática construir modelos formales o matemáticos que explican el razonamiento implícito en determinadas operaciones jurídicas.

Se habla así de una informática decisional para referirse a aquella parte de la informática jurídica capaz de llevar, sobre unos datos fácticos y normati-

vos previamente objetivados e incorporados a un lenguaje informático y a una base de datos, al acto de aplicación de la norma y a la decisión del caso concreto. A mi juicio, la dificultad –y la resistencia– de la sentencia a la total informatización del proceso discursivo-decisorio que realiza está representada por dos factores muy próximos entre sí: la interpretación de las normas y la valoración del sentido de lo justo.

La norma no es sólo escritura, o bien, en cuanto escritura, su función consiste en significar, y la significación no se obtiene a través de cualquier lectura, sino a través del acto de conocimiento que es la interpretación, por lo que únicamente una vez interpretada, puede decirse que existe la norma en cuanto tal. En definitiva, la norma es el resultado de su conocimiento a través de la interpretación y a partir de la escritura. Pues bien, los ordenadores razonan, infieren y calculan, pero no interpretan. La interpretación, que no es sólo semántica y lógica, sino también psicológica y ética, parece reservada todavía en exclusiva al ser humano. Si es así, sólo caben dos posibilidades que son, como he dicho en otro lugar (El papel de la lógica y de la informática en la esfera jurídica, separata de la revista «Informática e Diritto», 1982): o bien reputar la solución informática como una lectura pegada a la literalidad que no supondría la realización del total proceso interpretativo, el cual vendría remitido a una fase ulterior en la que se reconsideraría la lectura o solución informática para corregirla o rectificarla; o bien, introducir en la memoria de los ordenadores las normas ya dilucidadas interpretativamente, con lo que la solución informática podría suponer un acercamiento entre el universo de las normas y el universo de los casos, aunque tampoco hubiera de reputarse como necesariamente definitiva la solución.

La concepción dogmática veía en la aplicación de la norma al caso una operación lógica bajo la especie de un silogismo en el que se identificaba la norma general como premisa mayor, se aislaba el caso concreto como premisa menor y por subsunción de éste en aquella, se deducía la conclusión consistente en predicar del caso concreto la consecuencia jurídica que la norma establecía con carácter general. Desde tal perspectiva, si se consiguiese una incorporación del conjunto de todas las normas a una base de datos y se pudieran traducir los hechos a un lenguaje lo suficientemente cerrado formalizado y homogéneo respecto del de las normas, respondiendo el lenguaje de aquéllas y el de éstos a una estructura común, basada en unos mismos elementos invariantes, sería posible establecer reglas de inferencia y procedimientos que condujeran a la decisión inherente al acto de aplicación. De hecho, la informática jurídica, como disciplina científica, proporciona modelos muy simples de procedimientos semejantes, y, aunque estén muy lejos de servir para automatizar la aplicación del Derecho, ni siquiera en los casos más sencillos sí sirven para explicar en términos formales algunos procesos racionales implícitos en el razonamiento jurídico.

Sin embargo, todos los intentos de formalizar y automatizar la aplicación de las normas parecen tropezar con un escollo insalvable: la interpretación de las normas. Porque si bien hay expedientes de interpretación (o acaso de aplicación) que tiene en sí el rigor lógico, como los argumenta a maiore ad minus o a fortiori o, llevado al extremo, el propio razonamiento por analogía, hay operaciones interpretativas que parecen irreductibles a elementos lógicos.

La interpretación misma no consiste en quedarse a solas con la norma y dilucidar el conjunto de sus posibles sentidos bajo ciertas condiciones. Si ello fuera así, bastaría con crear una base de datos ingente e introducir en ella, para cada enunciado normativo el conjunto de todos los subenunciados en que aquél puede concretarse o especificarse. La interpretación requiere enfrentar la abstracción o la generalidad de la norma con la concrección del caso concreto o, al menos, con la relativamente mayor concrección de los enunciados en los que se contiene la descripción de un caso al que aplicar aquélla. Por esa razón, la interpretación de una norma no es nunca del todo predeterminable a priori y resulta sumamente difícil, por no decir imposible, procesar informáticamente un corpus de interpretaciones posibles para una norma dada. Todo lo más, podrá enfrentarse la norma con algunos supuestos imaginarios que, por hipótesis, se consideran como casos posibles respecto de los cuales decidir el sentido del precepto jurídico. Pero la infinita riqueza de la realidad de las relaciones sociales haría quebrar siempre el esquematismo de la previsión. De ahí los límites, al menos en el día de hoy, de ese aspecto de la informática jurídica que llamamos informática decisional.

La Escuela Histórica del Derecho, en el primer tercio del siglo pasado, impulsó la jurisprudencia a la primera fila del pensamiento científico tomando dos modelos: el de la historia natural y su base organicista desde la que el Derecho se presentaba como un sistema autorregulado y con una determinada orientación finalística; y el de la lingüística historicista desde la cual el derecho aparecía, al igual que el lenguaje, como una enamación cultural del volkgeist, y, como el lenguaje poseía unas reglas y una estructura universal en la que los juristas de todas las épocas y todos los países se reconocían. La idea de totalidad sistemática con «vida propia» de los organismos y la metáfora del lenguaje. Hoy la informática jurídica retoma, actualizándola, esa tradición en cuanto se dirige a la búsqueda de lenguajes artificiales y sistemas de conservación y tratamiento de información, que se expliquen, y remedien, la inabarcable diversidad diaria de la producción jurídica.

4.–La informática como objeto del Derecho

Existe un tercer aspecto de las relaciones entre la informática y el Derecho del cual el presente Congreso se va a ocupar muy especialmente aquí solo incidentalmente: la informática como objeto del Derecho.

El desarrollo de los equipos y procedimientos informáticos ha dado lugar a una nueva clase de bienes, o, en plural, a nuevas clases de bienes, que

pueden ser objeto del Derecho de la contratación, quizás también de alguna forma de propiedad especial, y, en todo caso, del tráfico jurídico, entendiendo por bienes todo aquello que puede ser objeto del tráfico jurídico y susceptible de protección por el Derecho.

La tradicional distinción romana entre las res corporalis y la res incorporalis, como suma divissio de los bienes comienza a quebrar aquí. Los programas de ordenador, el software, las aplicaciones, o las bases de datos construídas como aplicación de aquellos programas o conjuntos cada vez mayores de información, constituyen una mezcla de bienes materiales o corporales, puesto que el soporte físico siempre existe, y de bienes incorporales, representados por las formas de ordenación, los pasos de la programación en un determinado lenguaje de programación, y la propia información introducida.

El ordenamiento jurídico tiene tanto que tutelar los derechos sobre tales bienes frente a la utilización o a la apropiación indiscriminada de terceros, como regular la transmisión de los derechos que recaen sobre ellos o las nuevas formas de contratación relativas a los mismos.

Es un reto para las viejas categorías dogmáticas que, en algún caso, no parecen soportar fácilmente su aplicación a estos nuevos bienes. Así la ya problemática distinción entre los Derechos reales y los Derechos personales pierde la escasa nitidez de sus contornos. El denominado deber general de abstención adquiere matices distintos ante la esencial reproductibilidad y multiplicación de estos bienes. Dentro del tipo de tutela propio de la propiedad industrial o de la propiedad intelectual, hay limitaciones físicas para el posible registro de la propiedad de bienes informáticos. Como consecuencia de las redes informáticas intercomunicadas, no sólo el acceso a estos bienes puede producirse con facilidad sino que, en muchos casos, es imposible detectar que se ha producido. Y qué decir de la susceptibilidad de la posesión como instituto jurídico destinada a proteger el status quo, el mantenimiento del orden pacífico de las cosas en un campo en el que las alteraciones de ese orden pacífico transcurren en el interior de unos sistemas cerrados con el impulso de la corriente eléctrica, inadvertidamente.

El profesor Losano ha dicho que la historia del Derecho «está condicionada por las tres revoluciones de la escritura, de la imprenta y de la ordenación electrónica de los datos». En las tres revoluciones el Derecho es afectado a través del lenguaje. En la primera se pasa de la expresión oral a la escrita; en la segunda, de la escritura manual a la impresa y en la tercera, de la escritura tipográfica, impresa o mecánica al lenguaje tratado electrónicamente. Sobre todo en la informática decisional, se da otro paso que va del lenguaje natural al lenguaje artificial o simbólico.

Las tres revoluciones, lejos de ser contradictorias, tienen unidad de sentido. Cambia, en efecto, algo extrínseco, respecto del Derecho, como es la forma de recoger sus enunciados en la escritura, la imprenta y la informatiza-

ción. Sin embargo, pese al carácter exógeno de la transformación, ésta se proyecta sobre el propio contenido ordenador y el modo de cumplir sus funciones. Se trata siempre, con apoyo en técnicas muy distintas, de hacer más indelebles los datos jurídicos. El perfeccionamiento gradualmente conseguido redunda en una enunciación más correcta que, a su vez, depara mayores posibilidades de comunicación, lo que se traduce en la certeza del ordenamiento jurídico y en la asequibilidad de las soluciones a obtener con base en el mismo.

NOTA: El Comité Organizador no se identifica con las opiniones emitidas por los comunicantes y asistentes que aparecen en la presente publicación.

ACTAS (VOLUMEN I)

SESION I

MESA N.º 1.–PROTECCION DE DATOS I (ASPECTOS GENERALES)

Informática: el abuso de su poder

JORGE OSCAR ALENDE

Subdirector del Sistema Argentino de Informática Jurídica.
Director del Instituto de Informática y Derecho del Colegio de Abogados de Lomas de Zamora
(ARGENTINA)

INTRODUCCION

Así como un arma puede servir para ejercer la más legítima defensa o perpetrar el delito de homicidio, así como una sustancia química puede servir para curar o matar, la informática no es ni buena ni mala en sí misma. Del uso que de ella se haga, dependerá que el resultado sea beneficioso o dañino.

El avance tecnológico, que ha alcanzado en nuestro siglo una velocidad vertiginosa nunca registrada en cinco mil años de historia escrita, ha colocado en manos del hombre la herramienta más poderosa de las que hasta hoy se ha tenido noticia: la computadora. Creer que su utilización habrá de ponerse desinteresadamente al servicio del bien común constituye un ingenuo error. Ese avance tecnológico, lamentablemente, no ha sido acompañado por una evolución semejante en los terrenos de la ética y de la solidaridad social.

Los I y II Congresos, celebrados en Santo Domingo y Guatemala, fueron ámbito propicio para que conjuntamente con otros miembros del Sistema Argentino de Informática Jurídica, informáramos sobre la existencia primero, y los adelantos después, que en materia de informática jurídica documental habíamos alcanzado en la esfera del Ministerio de Justicia de la Nación Argentina.

Hoy, volvemos a informar en otro trabajo presentado en éste III Congreso Iberoamericano de Informática y Derecho, sobre los nuevos avances y el estado actual del SAIJ.

Pero además, al haber sido convocada esta reunión bajo el lema de «Nuevas Tecnologías y Libertades», no resisto la tentación de efectuar algunos comentarios a título personal sobre dos temas que merecen especial consideración por el peligro que una dañina utilización del recurso tecnológico que hoy nos congrega implica y que en forma amenazante se cierne sobre sociedades e individuos.

El primero, es el del flujo de datos transfrontera, es decir, el de la problemática generada por la transmisión internacional de la información por medios telemáticos y satelitales.

El segundo, el relativo a los datos personales, en especial aquellos denominados «sensibles», que el hombre desea mantener en la esfera de su intimidad, impedir que se utilicen para fines ilícitos o se conviertan en herramienta útil para la opresión.

Paso a tratarlos por separado, para luego formular algunas consideraciones finales.

FLUJO DE DATOS TRANSFRONTERA

Definición

Debo ante todo aclarar que existiendo gran cantidad y variedades de definiciones del concepto de «flujo de datos transfrontera» (FDT), en este trabajo dará al mismo un sentido amplio, entendiendo que en él tiene cabida todo tipo de transmisión, circulación, salida o emisión de información a través de las fronteras de los Estados, tratada o destinada a ser tratada por computadoras y/o en medios magnéticos y/o capturada o enviada por satélite, o transportada en cualquier soporte y destinada a ser consultada, procesada y/o almacenada.

La problematica

Aquellos avances tecnológicos a los que me he referido más arriba, en materia de telemática [1], permiten vaticinar que marchamos, a la velocidad de los fenómenos exponenciales, hacia un mundo no sólo totalmente informatizado, sino también totalmente interconectado, comunicado, en el que toda la información estará a nuestra disposición y al alcance de nuestra mano (o de nuestro computador). Esta facilidad con la que la información transita a través de las fronteras de los Estados, trae aparejada una serie de problemas

[1] Mientras hispanoparlantes y franceses continuamos disputando sobre la paternidad del término, en éste trabajo simplemente lo utilizaré para denominar a la exitosa unión de la informática con las comunicaciones.

económicos, políticos y jurídicos que se ven agravados por la imposibilidad de ejercer controles efectivos sobre ese flujo informativo.

En general desde los centro de poder de los países más desarrollados, invocando disposiciones constitucionales y principios, tratados y declaraciones sobre derechos humanos (derecho a la información), se brega por la libre circulación de la información. Por otra parte, desde los países menos desarrollados, al advertir el efecto perjudicial que sobre sus economías produce el procesamiento en los bancos de datos de aquellos centros de poder de la de información originada en sus propios territorios, oponen reparos al principio de la libre circulación que, expresan, debe ejercitarse en interés de todos y no solamente de quienes han capturado la información.

Ya en 1973 una ley sueca estableció que «la transferencia de datos para su procesamiento en el extranjero podrá efectuarse sólo tras autorización especial». El mismo año, en Málaga-Torremolinos, la Convención Internacional de Comunicaciones establecía el principio según el cual «los flujos transfronteras deberán efectuarse entre los países firmatarios sin ningún impedimento o interrupción y bajo condiciones de seguridad...». Tal como expresa Frosini, he aquí los dos primeros antecedentes de la diferencia de principios e intereses: mientras la ley sueca impone una barrera, la Convención recomienda un libre flujo de los FDT. [2]

Cabe aclarar que la preocupación que llevó a Suecia a la sanción de la ley referida, se centró en la circulación de información vinculada al derecho a la intimidad, al que me referiré más abajo; y cabe adelantar, que desde el punto de vista de los países menos desarrollados, la problemática se centra en torno al concepto de soberanía.

Clasificación de los FDT

Varias son las clasificaciones de que han sido objeto los FDT.

En el Documento de Trabajo TDF 200 preparado por la Oficina Intergubernamental para la Informática (I.B.I.) para la «Segunda Conferencia Mundial sobre Políticas de Flujo de Datos Transfronteras» que se reuniera en Roma en 1984, se ensaya una clasificación que contribuye a distinguir las distintas implicancias económicas de los mismos:

a) Flujos de Información científica y técnica.
b) Flujos de Información económica y social.
c) Flujos de Información educativa y cultural.
d) Flujos de Información comercial y financiera.
e) Flujos de Información administrativa.
f) Flujos relativos a la seguridad y la información.

[2] Frosini, Vittorio. «FDT ¿Barreras o Flujos Libres?», en el dossier núm. 8 de la Revista «Agora» «Soberanía e Informática», pág. 50 y sig.

Se han ensayado otras clasificaciones que han tenido en cuenta por ejemplo los medios de transmisión (electrónicos y no electrónicos) o la naturaleza de la relación (redes cerradas, ventas de servicios, venta o licencia de software o transacciones intrafirma). [3]

Estas clasificaciones, en general, ayudan para diferenciar la problemática que cada tipo de FDT acarrea y, en consecuencia, visualizar las soluciones que cada una de ellas requiere, que en algunos casos, podrán ser técnicas y en otros estarán relacionadas con las políticas informáticas que se adopten.

Entrar en ese análisis pormenorizado que precise o propicie soluciones puntuales para cada una de las distintas categorías señaladas, excedería las lógicas limitaciones impuestas a los trabajos que se presenten en este III Congreso Iberoamericano de Informática y Derecho, al mismo tiempo que también excedería mi modesta capacidad personal debido a la multiplicidad y variedad tipológica de las soluciones requeridas, señalada más arriba.

Deseo sí, efectuar algunos comentarios sobre cierto tipo de FDT, en especial los comprendidos en los puntos b) y f) de la definición vertida en el Documento de Trabajo TDF 200 de la I.B.I., que se encuentran intimamente vinculados al tema de la seguridad de las naciones y el ejercicio de los poderes soberanos que las mismas ejercen sobre sus recursos naturales.

La Cuestión de la Soberania

En la actualidad, algo más de tres mil satélites manejan la economía mundial. Indican la localización de las riquezas (aún) cuando se trate de yacimientos subterráneos), transmiten imágenes y sonidos, e intercambios telefónicos, computadores y bases y bancos de datos.

La dependencia de la economía mundial del sistema satelitario es tal, que si éste dejase de funcionar, «dejaría de funcionar» el planeta. Muchos de estos satélites están situados en órbita polar, pasando varias veces por día sobre los dos polos y reconociendo en cada nueva pasada una nueva zona terrestre, merced al movimiento de rotación del planeta. Otros, también dedicados a la observacion, están ubicados en la órbita heliosincrónica», lo que les permite pasar todos los días por el mismo lugar y a la misma hora.

La información que recogen unos y otros es de altísimo valor, ya que hoy, conocimiento, información, tal como lo expresa Tofler en su último libro, son sinónimos de poder: «... el conocimiento en sí es poder».[4]

En diciembre de 1962, las Naciones Unidas sancionaron una resolución relativa a la «Soberanía Permanente de los Estados sobre sus Recursos Natu-

---

[3] Ver Documento de Trabajo TDF 200 del I.B.I. para la Segunda Conferencia Mundial sobre Políticas en FDT, y Correa, Carlos y Otros, «Derecho Informático», Editorial Depalma, 1987, Buenos Aires.

[4] Toffler, Alvin, «El Cambio del Porder», Plaza y Janes Editores, 1990, Barcelona, España.

rales», que fue recogida en numerosos documentos de tipo diverso, y que proclama ámplios derechos a favor de los Estados dueños de tales recursos.

En ella se expresa que «El derecho de los pueblos y naciones a la soberanía permanente sobre sus riquezas y recursos naturales, debe ser ejercido en el interés del desarrollo nacional y del bienestar de la población del estado. La exploración, el desarrollo y la disponibilidad de dichos recursos, así como la importación de capitales extranjeros requeridos a este fin, deberían efectuarse de conformidad con las normas y condiciones que los pueblos consideran necesarias o convenientes respecto a la autorización, la restricción o la prohibición de dichas actividades.» Al referirse más adelante a las obligaciones de los inversores y de los países huéspedes de repartir los beneficios sobre el capital, establece que sus actividades deben desarrollarse en el marco de las «medidas necesarias para asegurar que, por ninguna razón, se perjudique la soberanía del Estado sobre sus recursos y riquezas naturales.[5]

Esta resolución fue recogida en numerosos documentos posteriores, dió origen a la resolución de 1974 sobre el «Programa de Acción para el Establecimiento de un Nuevo Orden Económico Internacional», y constituyó el principal antecedente para la formulación por parte del «Grupo de los 77», del «Código de Conducta de las Naciones Unidas para las Sociedades Transnacionales».

De acuerdo a este principio de la soberanía permanente, el poder soberano del Estado sobre sus recursos naturales se extiende a éstos aún después que hayan sido extraídos por las empresas extranjeras y a pesar de la existencia de acuerdos que establezcan lo contrario. La aplicación directa del principio a los FDT, tal como lo expresa Vittorio Frosini en el trabajo referido en [2], implicaría «que la soberanía también abarca, entre otras cosas, los datos sobre recursos minerales y naturales estratégicos almacenados en bases de datos, aún cuando éstas pertenezcan a compañías extranjeras y se encuentren en el exterior». Y se pregunta Frosini a continuación: «¿Se puede pretender la soberanía sobre detos de este tipo?».

En mi opinión, la pretensión parece teñida de chauvinismo y se encuentra superada por la realidad tecnológica. Pero... ¿no se lesiona de alguna manera la soberanía de un Estado, cuando desde dentro de su propio territorio, o desde su espacio aéreo, sin su permiso, control ni conocimiento, se envía hacia el exterior información sobre sus recursos naturales, o se toman fotografías satelitarias que serán, conjuntamente con los datos, procesadas y utilizadas para realizar transacciones o adoptar políticas que redundarán en perjuicio de los intereses de ese Estado del cual la información es originaria?.

El almacenamiento de datos relativos a los países subdesarrollados en los bancos de datos de los países desarrollados ha permitido a éstos la realiza-

---

[5] Resolución de las Naciones Unidas del 14 de diciembre de 1962.

[2] Frosini, Vittorio. «FDT ¿Barreras o Flujos Libres?», en el dossier núm. 8 de la Revista «Agora» «Soberanía e Informática», pág. 50 y sig.

ción de sus operaciones comerciales de los últimos años dentro de un marco de seguridad establecido especialmente por la desigual posibilidad de acceso a la información.

Las redes de comunicaciones de las potencias desarrolladas captan datos de todo tipo, que incluyen los referentes al subsuelo, al fondo del mar, a las áreas sembradas, a fenómenos meteorológicos, etc., etc., etc...; y toda la información recogida mediante el FDT es procesada por los poderosos «cerebros electrónicos» del mundo desarrollado, que pueden armar así un complicado rompecabezas en el que intervienen cálculos sobre la oferta y demanda, previsiones monetarias, análisis sociales, estrangulamientos presupuestarios y múltiples aspectos más.

Todo esto es más preocupante aún, al tomar noticia de que el ochenta por ciento, o tal vez más, de los datos que fluyen trasfrontera, son intra-empresa transnacional.[6] Es decir, que no se trata de transacciones producidas en el mercado abierto, o de información destinada a la ejecución de algún problema educativo o de ayuda económica a los países menos desarrollados. Es FDT puesto al servicio del fin de lucro que caracteriza a las actividades mercantiles.

Los FDT en la Republica Argentina

En la República Argentina no existen disposiciones legales referentes al tema que nos ocupa.

La realidad nos muestra una tendencia creciente a la transmisión de información mediante el correo electrónico y el facsímil, en detrimento de la utilización del télex y de los telegramas. Ya en 1987, enviar un mensaje de una página a los Estados Unidos de norteamérica por via telemática, resultaba treinta veces más rápido y cuarenta veces más barato que por vía télex. Estudios y encuestas revelan también que en ese mismo año el cuarenta y ocho por ciento de las empresas consultadas enviaban o recibían datos del exterior vía computadora, el treinta y cinco por ciento usaba facsímil y el veintiocho por ciento enviaba o recibía soportes magnéticos. Las consultas pusieron de manifiesto además que el crecimiento de estos porcentajes se operaba en forma más acelerada.[7]

Vemos pues, que a pesar de la desproporción existente en materia de poder informático instalado a favor de los países más desarrollados (más del noventa y cinco por ciento en el hemisferio norte y menos del cinco por ciento en el hemisferio sur) mi país, como todos los de la región, no es ajeno a la explosión informática, y que por lo tanto se deberá prestar al fenómeno especial atención, habida cuenta de la importancia de sus consecuencias.

* * *

[6] La Oficina Intergubernamental para la Informática (I.B.I.), estableció el porcentaje en el 82%. CARLOS CORREA y Otros, (obra citada en (3)), en el 80 %.

[7] CORREA, CARLOS y Otros, obra citada en (3).

LOS DATOS PERSONALES

Al igual que las sociedades menos desarrolladas pueden ver perjudicados sus intereses económicos y lesionadas sus soberanías, los individuos pueden ser también víctimas de la mala utilización del recurso informático, cuando éste es puesto al servicio de acciones que ponen en peligro sus derechos y hasta su libertad y su vida.

La historia, la vieja y la reciente, es un nutrido muestrario de casos en que los totalitarismos de las más variadas ideologías utilizaron la información como fuente del ejercicio del poder. El peligro se ha acrecentado en el mundo moderno, ya que el tratamiento automático de los datos multiplica sus posibilidades de procesamiento y utilización. Tal como expresara Fauvet [8] «la informática es un poder que da aún más poder a quien la domina».

La acumulación de datos personales en las bases de datos trae aparejada una doble consecuencia: crea una fuerte desigualdad entre los individuos según el cual es la posibilidad de acceso a los datos, por una parte, y amenaza afectar el derecho a la intimidad, por la otra.

Como lo expresa Novoa Monreal [9], al tratar este tema, nos encontramos frente a un fuerte conflicto de derechos. Por un lado, el derecho a la información, de jerarquía constitucional, ya que se caracteriza como el derecho de dar y recibir información que se fundamenta en la libertad de expresión que consagran la gran mayoría de las constituciones (art. 14 de la Constitucion Nacional Argentina), e integrante de los Derechos Humanos proclamados en la Declaración Universal de los Derechos del Hombre (art. 19) [10]. Por el otro, el derecho a la vida privada, que también tiene jerarquía constitucional (art. 19 de la Constitución Nacional Argentina) e integra asimismo los mencionados Derechos Humanos de la Declaración Unviersal (art. 12).

Ambos derechos, además, se encuentran reconocidos, en el ámbito europeo, por la «Convención de Salvaguarda de los Derechos del Hombre y de las Libertades Fundamentales», aprobada por el Consejo de Europa en Roma, el 5 de noviembre de 1950, y en el americano por la «Convención Americana por los Derechos Humanos» (Pacto de San José de Costa Rica), firmado el 22 de noviembre de 1969.

La búsqueda de soluciones legislativas al conflicto de derechos que nos ocupa registra ya varios años de existencia. Algunos países han incorporado normas concretas referidas al uso de la informática respecto de los datos

---

[8] FAUVET, JACQUES, presidente de la «Comisión Nacional de Informática y Libertades» de Francia, conferencia pronunciada en la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Buenos Aires, el 6 de mayo de 1987.

[9] NOVOA MONREAL, EDUARDO, «Derecho a la Vida Privada y Libertad de Información. Un Conflicto de Derechos», Edit. «Siglo XXI», Méjico, 1981.

[10] Declaración aprobada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948, complementada por dos pactos internacionales de 1966.

personales de carácter sensible. Quienes concurrimos hoy a éste III Congreso Iberoamericano, somos huéspedes de uno de ellos; en mi patria, varias modernas constituciones provinciales han consagrado idénticos principios. Otros países, han buscado soluciones a nivel legislativo.

Los últimos quince años han registrado una inmensa actividad legislativa en especial en los países industrializados, tendientes a lograr, a través de la utilización de distintas técnicas legislativas, regulaciones apropiadas en materia de datos personales. El año 1978 fue prolífico en la materia. Noruega, Dinamarca, Austria y Francia, dictaron leyes que se consideran como los ejemplos más acabados en materia de protección de informaciones sensibles.

De entonces a hoy, decenas de leyes y proyectos han ocupado al legislador, que ha plasmado en esos textos varios principios que han sido enunciados en numerosos trabajos y publicaciones [11]. En apretada síntesis, podemos resumirlos expresando que tienden a que los datos que se recolecten sean veraces y objetivos, que toda recolección tenga objetivos prefijados, propósitos generales y usos socialmente aceptables, que la información no se guarde por más tiempo que el necesario para alcanzar los fines perseguidos, que esa finalidad se encuentre especificada en el momento de la recolección, que se impida el acceso a los datos por parte de terceros, tomándose los recaudos de seguridad necesarios para evitar esos accesos, pérdidas o destrucciones, que se garantice la transparencia de los procedimientos, que exista un organismo de control y que se permita una amplia participación individual por parte del titular de los datos, que podrá así oponerse en casos de existencia de información errónea o incompleta.

LA SITUACION LEGAL EN LA REPUBLICA ARGENTINA

En mi país, si bien no se ha sancionado un texto legal específico, son varios los proyectos que se encuentran en trámite parlamentario y que obedecen, en líneas generales, a los principios enunciados precedentemente.

La normativa vigente, registra normas de distinto nivel jerárquico vinculadas con el tema.

Ante todo, la Constitución Nacional establece en su art. 19 que «Las acciones privadas de los hombres que de ningún modo ofendan al orden y la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados. ...». El artículo 18 de la misma, establece la inviolabilidad del domicilio, la correspondencia y los papeles privados.

---

[11] Ver por ejemplo LUCHETTI, AÍDA «Informática y Derechos Individuales», II Congreso Nacional de Informática Jurídica, Córdoba, agosto de 1987, o CORREA, CARLOS y otros, obra citada en (3).

Por ley nro. 21.173, se incorporó al Código Civil el art. 1071 bis, que expresa «El que arbitrariamente se entrometiere en la vida ajena publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado cesar en tales actividades si antes no hubiere cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuere procedente para una adecuada reparación».

Finalmente, en el Código Penal, los artículos 151 y 152 por una parte y 153 y siguientes por la otra, establecen penas para quienes cometan los delitos de violación de domicilio y violación de secretos respectivamente.

EVOLUCION CONCEPTUAL DEL DERECHO A LA INTIMIDAD

Antes de formular algunas consideraciones finales sobre los dos temas objeto de este trabajo, y a fin de completar aunque más no sea someramente, el panorama de la temática referente a los datos personales, considero necesario dedicar alguna atención a la evolución que ha sufrido a través del tiempo el concepto de derecho a la intimidad de los individuos.

Tal como lo expresa quien fuera mi maestro, el profesor WERNER GOLDSCHMIDT [12], el derecho a la intimidad fue clásicamente concebido como «the right to be alone», es decir, el derecho a ser dejado en paz, o a ser dejado solo, criterio que se originó a fines del siglo pasado, cuando WARREN y BRANDEIS publicaron un artículo que tuvo gran difusión, en la «Harvard Law Review». Mas como destaca FROSINI [13], esta concepción se encontraba cargada de un acentuado individualismo, propio de una época lejana en el tiempo y superada por la realidad.

Ya no se trata, en su criterio y en la actualidad, de una libertad aristocrática, sino de una libertad democrática. Como lo señala CORREA [14], citando a Rodotá, el problema no consiste en garantizar la opacidad de la vida privada sino la transparencia del accionar de las entidades públicas o privadas que se dan a la tarea de recolección de datos. El derecho a la vida privada no se concibe más en la actualidad como la libertad negativa de oponerse a ser objeto de recolecciones de datos que conciernen al individuo, sino que se ha convertido en la libertad positiva de supervisar el accionar de quienes recolectan y usan la información. Ya no puede el hombre moderno encerrarse detrás de un muro de ladrillos y pretender allí «ser dejado solo». Hoy, el muro es transparente, el ser humano se ha convertido en un «hombre de cristal», tal

[12] GOLDSCHMIDT, WERNER, «El Derecho a la Intimidad», El Derecho, T. 112, pag. 832.
[13] FROSINI, VITTORIO, «Banche dei Dati e Tutela della Persona», edit. Por la Cámara de Diputados de Italia, Roma, 1983.
[14] CORREA, CARLOS, ob. citada en (3).

como se expresara en una transcendente sentencia del Tribunal Constitucional Federal de Alemania.[15].

CONSIDERACIONES FINALES

La lectura de los temas a tratar en este III Congreso Iberoamericano de Informática y Derecho, en especial la contemplada en su primera parte «Derecho de la Informática», me sugirió proceder a la redacción del presente trabajo, con la finalidad de expresar en él una profunda preocupación.

El avance tecnológico ha alcanzado un ritmo de vértigo, y el poder informático, que tanto puede hacer en pro del ser humano, se muestra alarmantemente amenazante por las concretas posibilidades existentes a favor de quienes lo detentan, de ejercer un uso abusivo y opresivo del mismo.

¿Ha aprendido el ser humano a considerar el interés general por encima del interés particular? ¿Han aprendido, los hombres y los pueblos, a respetar a los hombres y los pueblos?

En mi opinión, no.

Ya adelanté, al inicio de este trabajo que, lamentablemente, «ese avance tecnológico no ha sido acompañado por una evolución semejante en los terrenos de la ética y de la solidaridad social».

Somos los dominadores del planeta, nos hemos impuesto a todas especies animales que lo habitan, pero lo hemos depredado, lo hemos contaminado, no hemos sabido imprimirle a su historia un rumbo mejor. No hemos sido capaces de encontrar para la convivencia social la paz y la organización de la colmena o del hormiguero.

La cotidiana lectura de los diarios, la televisión, la radio, nos bombardean permanentemente con noticias de guerra, crímenes, desordenes, corrupción. La explotación del hombre por el hombre sigue siendo la característica de muchas sociedades actuales; evidentemente, el comportamiento humano no ha variado mucho desde tiempos remotos; basicamente, el hombre ha seguido siendo siempre casi el mismo, mientras lo que variaba fue su entorno.

¿Es nuestra naturaleza la que nos lleva a comportarnos así? Si así fuere, pues tendremos que internalizar la convicción de la necesidad del cambio. Así como alguna vez levantamos nuestra cabeza, la alejamos del suelo, dejamos de caminar en cuatro patas y comenzamos, al tener otra visión de la realidad, a desarrollar nuestra inteligencia, debemos, para forjar un futuro mejor para la especie, utilizar esa inteligencia para alejarnos ahora de instintos primitivos que nos pueden llevar no sólo a un mundo injusto y opresor,

[15] LUCHETTI, AÍDA. Trabajo citado en (11).

sino al caos y a la desaparición. Cálculos científicos efectuados con modernas tecnologías y basados en el conocimiento que actualmente se posee del universo, han otorgado a la especie humana apenas algo más de un cuarenta por ciento de posibilidades de supervivencia dentro de los próximos cien años, si no variamos nuestros patrones de conducta.

La utilización que se efectúe del recurso informático respecto de los dos temas objeto de éste trabajo, debe necesariamente estar inspirada en la solidaridad social y en el respeto a los derechos individuales.

Con relación al flujo transfronterizo de datos, necesariamente, esa especial preocupación que debemos tener por su problemática desembocará en el tratamiento legislativo del tema, mas ello no será suficiente. Los tratados internacionales y las convenciones multilaterales también resultaran imprescindibles, ya que el carácter supranacional de la telemática torna ineficaz a la ley nacional como solución única del problema, que requiere el juego interactivo del derecho internacional.

El contenido de esas leyes e instrumentos internacionales, será el resultado de la confrontación de los intereses de la naciones y de las regiones en conflicto. No podrá limitarse al aspecto jurídico inspirándose en asépticas aspiraciones de justicia, sino que deberá considerar las serias implicaciones económicas, políticas y sociales que caracterizan al fenómeno informático en general, y al tema que nos ocupa en especial. Allí es donde el problema se torna candente, la paz y la justicia, reclaman de quienes tengan la responsabilidad de establecer las bases del futuro de la humanidad, que sepan estar a la altura que el momento histórico exige. Necesitamos un hombre mejor, capaz de transitar con altruísmo el camino de la vida, para poder así llenar de justicia la conducta y el derecho. Porque tal como se ha expresado en una reciente «Reunión de Expertos en Informática y Electrónica» celebrada en San Pablo, Brasil, «La informática está en la base de las profundas alteraciones en el mundo... no es neutra; o sirve al desarrollo o sienta las bases de una nueva y más profunda dependencia». Esa dependencia, en la sociedad tecnológica, puede llegar a tener visos de esclavitud.

Respecto al derecho a la intimidad y la protección de datos personales, la preocupación es similar. Sólo cambia la víctima, que en este caso es el individuo aislado.

Nuestra América latina es rica en ejemplos de abusos de información que permitieron tremendas violaciones de los derechos humanos.

El poder que confieren las modernas tecnologías a los centros recolectores de información excede los límites de lo imaginable. Si en países de escaso desarrollo, puede extraerse una detallada radiografía de la vida privada de un individuo, con sólo reunir la información que se posee sobre su persona en los registros de bienes inmuebles, automotores, aeronaves y demás bienes muebles registrables, mas la contenida en entidades bancarias y financieras,

las contenidas en las empresas de transportes aéreo, naval y terrestre, etc. etc., ¡cuan tremendo que podrá ser el poder informático de aquellos países que merced a su desarrollo económico están en la avanzada de la producción de hardware y software!.

Por otra parte, el avance tecnológico torna cada vez más fácil el procesamiento de la información, más sencillas y baratas las comunicaciones y más poderosos los equipamientos informáticos, al punto que todo el potencial de una computadora de la década del 60, que requería de grandes espacios para su instalación, puede llevarse hoy en un bolsillo, mientras se ha avanzado tanto en materia de velocidad de procesamiento que procesadores trabajando en paralelo pueden ser capaces de funcionar a muchos millones de MIPS.

Para enfrentar este futuro tan revolucionado como peligroso, la humanidad requiere estar compuesta por hombres mejores, imbuídos de un espíritu solidario que se alce sobre el egoísmo y el sectarismo.

La informática, que forma ya parte de todas y cada una de las actividades del ser humano, sigue avanzando al ritmo de los fenómenos exponenciales, que el hombre no es capaz de percibir intuitivamente, y cada vez más, la posesión del poder que ella implica se asemeja a la figura de un niño jugando con un arma mortal.

Bruno Lussato, en una obra destinada a poner de manifiesto similares preocupaciones a las que expongo en este trabajo [16], expresó: «Resulta evidente que este libro no pretende ser imparcial, sino que, muy por el contrario, toma abierto partido por estar asentado en convicciones. Son estas, el lector lo habrá advertido facilmente, las de un hombre profundamente liberal que siente verdadero pánico ante la burocracia y la alienación, que por encima de todo tiene apego a la libertad, y que sigue siendo, a pesar de todo, optimista con respecto a la naturaleza humana».

Las preocupaciones, repito, las comparto. Envidio su optimismo respecto de la naturaleza humana.

A los hombres de derecho, y en especial a quienes estamos vinculados a los problemas de la informática, nos cabe una gran responsabilidad: consistiendo nuestra principal actividad en el estudio de la conducta del hombre, debemos crear conciencia, ante el peligro, de la necesidad de crear nuevas pautas de comportamiento, nuevas normas de convivencia, para poder así dejar un mundo mejor a nuestros hijos. La informática, debe estar al servicio de esta idea, debe convertirse en la herramienta que favorezca el acercamiento y el entendimiento mutuo entre las naciones y el respeto al ser humano, sea cual fuere su ideología, su raza o religión.

Que así sea.

[16] LUSSATO, BRUNO «Le défi Informatique», Librairie Artheme Fyard, 1981.

Intimidad personal y limitaciones

M.ª DEL CONSUELO BLÁZQUEZ DE ANDRÉS
Estudiante de Derecho en la Universidad de Extremadura

VALENTÍN CARRASCOSA LÓPEZ
Doctor en Derecho. Licenciado en Ciencias de la Información.
Director del Centro Regional de Extremadura de la U.N.E.D.
Secretario Judicial. Graduado Social
(ESPAÑA)

Ni que decir tiene que la intimidad personal, harto definida por la doctrina, es lo de uno mismo, lo más profundo, lo más sentido; ese derecho que tiene la persona por el mero hecho de serlo, un derecho fundamental proclamado en nuestra Constitución en el artículo 18.1 que garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen, así también en la L.O. 1/1982 de 5 de Mayo, entre otras. Por ello, viviendo en una sociedad que proclama y garantiza los derechos fundamentales, ¿hasta qué punto se puede limitar un derecho fundamental inherente a la persona, o dar prioridad a uno de estos derechos respecto a otros?.

Si bien la libertad informativa es también un derecho fundamental, reconocido en el Artículo 20.1 de la Constitución, el mismo artículo en su párrafo cuarto limita esta libertad en el respeto a los derechos reconocidos en este título –«De los derechos y deberes fundamentales»–, y el artículo 18.4 que estipula como es sabido, que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Igualmente el artículo 7 del Código Civil limita la utilización del derecho cuando éste sobrepase los límites normales

de su ejercicio con daño para tercero, dando lugar a la correspondiente indemnización y a la adopción de medidas judiciales o administrativas que impidan la persistencia en el abuso. A mayor abundamiento, por ejemplo, la sentencia del Tribunal Constitucional del 14 de Febrero de 1992 sienta como fundamento del fallo la doctrina de que la intimidad personal debe prevalecer frente a la libertad informativa. Y en esta línea LASARTE ALVAREZ [1] afirma que la mera curiosidad o el entrometimiento en las parcelas de la vida ajena que el interesado ha preservado del conocimiento público no justifica la divulgación de dato alguno, aunque sea veraz y fácilmente contrastable.

Con ello pretendemos, como se puede dilucidar, que si bien la informática –información automática– viene a ser un bien público en beneficio de todos que contribuye al avance y al progreso tecnológico, no es base para limitar, restringir, o menoscabar arbitrariamente el ámbito de lo privado, de lo íntimo. Se habría logrado un triunfo a un precio muy alto, porque como decía LÓPEZ GUERRA... [2] «Si un sistema democrático es preferible, es precísamente porque garantiza los derechos de cada ciudadano y de todos ellos, y esta garantía debe alcanzar a aspectos tan decisivos en nuestra cultura, y tan arraigados en nuestra forma de ser y vivir como son los llamados derechos de la personalidad: la intimidad personal y familiar, la propia imagen, el honor...». Siguiendo esta pauta de garantías de derechos fundamentales, y por lo tanto, de protección de datos personales, hay que señalar que la única norma que tenemos en la actualidad y que fue firmada y ratificada por España, es la del Convenio Europeo de Protección de Datos. Quien nos hace partícipes de la necesidad de ampliar las garantías de los derechos y libertades fundamentales, y en concreto, el derecho a la INTIMIDAD, teniendo en cuenta la intensificación de la circulación internacional de los datos de carácter personal que son objeto de tratamientos automatizados. Este Convenio ha representado el primer Tratado Internacional suscrito por España, sobre protección de la intimidad personal ante la utilización de datos personales en ficheros de tratamiento automático. Sin embargo el artículo 4.1 de referido Convenio estipula que «cada parte adoptará en su derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos enunciados en el presente Capítulo». Con lo cual, aunque España haya ratificado este Convenio, si no introduce en su ordenamiento un conjunto de normas que den viabilidad a lo acordado y ofrezcan sobradas garantías, de poco le habrá servido. Esperemos que el Proyecto de Ley Orgánica de regulación del tratamiento automático de datos personales, en su resultado final y una vez enmendada consiga los objetivos deseados, así como proclamaba la Comisión francesa de Informática y Libertades, DOMINAR no paralizar la informática.

---

[1] LASARTE ALVAREZ, C.: Revista Tapia, Año XI, Núm. 64.

[2] LÓPEZ GUERRA, «Protección de los derechos fundamentales y libertades públicas», Número VI, 1989. Cáceres.

Ahora bien, por otra parte, creemos imposible delimitar estrictamente el derecho a la intimidad: primero, porque el concepto de intimidad varía de uno a otro; segundo, porque lo que hoy constituye «intimidad personal» quizás antaño no lo fue y tercero, porque en el futuro, probablemente, se tendrá una idea diferente de la que hoy tenemos. Sin embargo, es evidente, que en un Estado Social y Democrático de Derecho, no cabe una mala utilización de las masas de datos de cada individuo que se encuentran almacenadas en los ordenadores, su descontrol, porque entonces nos sumerigiríamos en un caos, en un retroceso irreparable. De forma que si el derecho a la intimidad personal queda limitado en pro de fines comunes, legales y necesarios exigiendo para ello a los ciudadanos su apoyo y contribución, igualmente estos han de disponer de sus propias informaciones, ejerciendo una labor de inspección, correción y de salvaguarda de sus propios datos. Y así, si a través de la Informática y para obtener unos determinados resultados, que se supone o no puedan resultar fructíferos, inadecuadamente se viola la intimidad personal de un sujeto, se estará empleando el derecho a la libertad de información para burlar el derecho a la intimidad personal, siendo prioritario totalmente este frente a aquel. Y es que como decía HEREDERO HIGUERAS [3] «...El problema de los datos registrados en soporte informático no es ese, sino el de la posibilidad de la adopción de decisiones por parte de las Administraciones públicas o entidades privadas, que afecten a un individuo en su esfera personal, laboral, profesional, etc., merced a refinados procesos de inferencia automática y de predicción de conductas... Cada vez más la información de carácter personal constituye un bien objeto de tráfico comercial y como tal, es materia prima de determinadas actividades mercantiles... La información personal se convierte así en algo intangible y que escapa al dominio del interesado...»

Un caso muy reciente, y que viene a colación con nuestro tema, aunque no se trate de información automatizada pero sí de otro medio de obtener información y que atacó a un derecho fundamental –intimidad personal– es el conocido y llamado «caso Naseiro». Así en el auto sobre este hecho de fecha 18 de junio de 1992, de la Sala Segunda del Tribunal Supremo, en la que fue Ponente el Excmo. Sr. Ruiz Vadillo, merecen destacar, entre otros, dada su vital y considerable importancia los siguientes datos:

– En el fundamento de derecho primero [4] se afirma que ...» No se puede obtener la verdad real a cualquier precio. No todo es lícito en el descubrimiento de la verdad. Sólo aquello que es compatible con la defensa del elemento nuclear de los derechos fundamentales, así la dignidad, la INTIMIDAD, etc., dentro de los parámetros fijados en la Ley..., hay que recordar

[3] HEREDERO HIGUERAS, M.: «La protección de los datos personales registrados en soportes informáticos». Revista de actualidad jurídica e informática. Ed. Aranzadi, N.º 2. Enero de 1992.

[4] Auto de la Sala Segunda del Tribunal Supremó de fecha 18 de junio de 1992. Madrid.

que uno de los presupuestos fundamentales de nuestro Estado de Derecho, democrático y social, establecido en la Constitución, es el del respeto a la dignidad e intimidad de la persona, esencialmente libre...». Con ello, este Tribunal plasma de una forma magistral la prioridad del derecho a la intimidad, que ha de servirnos de pauta y apoyo a todos los ciudadanos, así como de escudo y defensa ante todas las intromisiones y limitaciones ilegítimas de los derechos fundamentales. No queremos decir con esto que haya que esperar el ataque para formular la defensa, porque lógicamente lo ideal sería una práctica preventiva que no represiva, pero para todos aquellos casos que forman ya un presente palpable y para los que se puedan dar inevitablemente, esta resolución constituye una buena defensa que no hay que olvidar.

– El fundamento de derecho segundo (4) recoge que...» en las situaciones que ahora se contemplan está en juego uno de los derechos constitucionales más importantes, como ya se dijo: el derecho a la intimidad en uno de sus componentes más interesantes... la intimidad es, probablemente, el último y más importante reducto, con el derecho a la vida, a la integridad y a la libertad de la persona humana, de las mujeres y de los hombres todos..."

¿Y acaso no es sorprendente, indignante y vergonzoso que en una sociedad, tal la nuestra, supuestamente garantizadora de los derechos fundamentales de la persona, se pongan en juego estos mismos derechos?. Si efectivamente nos encontramos inmersos en un mundo de derechos y libertades, de tecnologías, de garantía y seguridad jurídica, es intolerable el avance y el retroceso al mismo tiempo. Y es que si el campo informático comporta una serie de beneficios, un progreso de hoy y para el futuro, no es admisible que, en su consecuencia, y al mismo tiempo se tambaleen o «bailen en la cuerda floja» el peso y los cimientos de un Estado que a través del esfuerzo y del tiempo han ido forjando consistentemente los derechos humanos.

– En el fundamento de derecho cuarto (4) se recoge «la necesidad de rodearse de las correspondientes garantías para evitar limitaciones injustificadas en los derechos fundamentales y libertades públicas que tienen un valor central en el sistema jurídico..."

Necesidad inminente que el legislador ha de preveer y positivizar, en base a un conjunto de normas taxativas no sólo de protección de datos personales registrados en soportes informáticos, si no que ofrezcan las suficientes garantías como para tener la tranquilidad que el uso de la informática no atentará contra la intimidad de las personas ni limitará injustificadamente sus derechos fundamentales. Y para el supuesto que en determinados casos así fuere, tipificarlo en el Código Penal como delito concreto y específico para estas violaciones y «atar todos los cabos» con una precisión especial que asegura al ciudadano que ante todo y sobre todo privan sus derechos fundamentales, así el derecho a la intimidad.

Que tenga la confianza y la seguridad que ni el Estado ni un particular ajeno manejan datos de su vida privada, de su intimidad, a su antojo.

Queremos hacer un llamamiento desde aquí y en la medida de nuestras posibilidades a todos los ciudadanos para que estén alerta y luchen con nosotros por una regulación exhaustiva del uso de la informática en todo su ámbito, y ello porque es una cuestión espinosa que puede hacer temblar la base de un Estado social y Democrático de Derecho provocando no pocos conflictos tanto a nivel internacional, como nacional y, en consecuencia, individual, lo cual ha de estremecer a cualquiera persona con un mínimo de sensibilidad.

Derecho a la intimidad y publicidad de datos personales de carácter patrimonial

ALFONSO DE JULIOS CAMPUZANO ESPAÑA

Licenciado en Derecho. Universidad de Sevilla. Profesor asociado del Dpto. de Filosofía del D.º, Moral y Política de la Universidad de Sevilla desde noviembre de 1990 hasta abril de 1992. Imparte docencia en la Facultad de Derecho de la asignatura D.º Natural, y en la Facultad de Informática de Derecho de la Informática

(ESPAÑA)

La aparición de la informática y su extensión a todos los órdenes de la sociedad ha traído consigo una fuerte conmoción de las estructuras sociales existentes. La sociedad post-industrial de nuestra centuria ha dejado paso a la sociedad informatizada o sociedad de la información que destaca como aspecto esencial de la misma el tratamiento masivo de la información como fuente de poder y riqueza. Es obvio que la información ha devenido el símbolo emblemático de nuestro tiempo.

La irrupción del fenómeno informático ha traído consigo la vulnerabilidad de las libertades del individuo y la invasión frecuente de su esfera privada. El concepto de un ámbito privado que se sustrae a la interferencia de otros tiene su origen en el nacimiento de una nueva forma de libertad y en la aparición de la persona como ente autónomo capaz de regir su propia vida. La intimidad, el ámbito íntimo, o la privacy, por utilizar la terminología anglosajona, es un concepto moderno que alcanza un reconocimiento implícito, a través de la libertad de conciencia, en las declaraciones de derechos

que se promulgarían con el advenimiento del Estado liberal y tendrá su reflejo en la tradición constitucionalista occidental de nuestro siglo.

Sin embargo el derecho a la intimidad ha dejado de ser un status negativo para convertirse en un status positivo. La invasión de la vida privada de los ciudadanos por parte de otros agentes sociales, públicos o privados, y la colisión de este derecho con otro igualmente protegible, el derecho a la información, sitúa a la intimidad como derecho ejercitable activamente. La garantía de su efectividad vendrá dada por la posibilidad de control activo y directo de los ciudadanos sobre el caudal de información que puede afectarles.

A la luz de todo ello, el derecho a la intimidad adquiere una configuración distinta en la sociedad tecnológica de nuestros días: el flujo de informaciones y de datos personales invade todas las esferas del actuar individual, y el individuo, desbordado por tan incontrolable avalancha tecnológica corre el riesgo de perecer víctima de la carrera denodada por el progreso.

El derecho a la intimidad, tradicionalmente definido como un derecho esencialmente negativo, adquiere en la actualidad perfiles nuevos y distintos: ya no se tratará de un derecho delimitador de un ámbito de no interferencia, sino que vendrá a definirse con un contenido abiertamente positivo. Frente al derecho a la información, caracterizado por su doble vertiente de derecho a informar y a ser informado, el individuo de la sociedad tecnológica afirmará su derecho primario a controlar el flujo de informaciones que sobre su vida privada puede existir en los bancos de datos. La intimidad se perfila así como derecho o facultad de autodeterminación informativa y encontrará su expresión legislativa a nivel internacional en el Convenio Europeo para la Protección de datos personales.

Sin embargo, esta facultad de autodeterminación puede colisionar en alguna medida con otros bienes jurídicos protegibles. La intimidad no es, no puede ser, un derecho absoluto ni una prerrogativa inviolable. El ordenamiento jurídico prevé cauces adecuados para la tutela de todos los bienes jurídicos protegibles y articula los mecanismos para la ponderación de los mismos en caso de conflicto entre dos o más de ellos.

En el ámbito mercantil la intimidad y el secreto de las operaciones financieras se ha visto con frecuencia vulnerado en virtud del primado de un bien jurídico superior: la seguridad del tráfico mercantil o el interés recaudatorio de la Hacienda Pública son un buen ejemplo de ello. En el segundo supuesto la jurisprudencia ha venido a ratificar el primado del interés público sobre el secreto bancario de depósitos, cuentas corrientes y otros activos financieros.

En el primer supuesto, la seguridad del tráfico mercantil urge la publicidad de determinadas operaciones financieras y aconseja su inscripción en el Registro Mercantil como medio adecuado para asegurar el buen fin de las mismas.

Es evidente que el buen fin de las operaciones y la seguridad del tráfico debe actuar como principio corrector de la privacidad de las situaciones patri-

moniales y de las operaciones financieras cuando éstas pueden afectar los intereses de terceros.

Pero lo que no queda tan claro, por lo dicho, es que esta función correctora pueda quedar al arbitrio de agencias privadas que intervegan como «mediadores» en el mercado financiero, ofreciendo sus bancos de datos como medio para asegurar la solvencia de los agentes financieros.

El hecho a que hacemos referencia tiene su reflejo en una situación de actualidad que, a buen seguro, no habrá pasado inadvertida para aquellos que somos sensibles a estas cuestiones: el anuncio de una conocida agencia de cobro de impagados por el que se pone a disposición del público en general sus bases de datos ("El Cobrador del Frac hace pública su base de datos").

La cuestión es en sí lo suficientemente sintomática como para reclamar una lectura detenida del acontecimiento. No podemos olvidar que la invasión del ámbito de lo privado, su confinamiento a límites cada vez más definidos, y la prevalencia de la información como bien de consumo en la sociedad tecnológica contemporánea ha contribuido a perfilar una nueva noción de intimidad más acorde con la demanda creciente de información en la sociedad informatizada.

En este sentido conviene destacar que el origen del proceso de acopio de datos que constituye la característica definitoria de nuestro tiempo responde a una necesidad creciente del Estado moderno en su compromiso material con la mejora de las condiciones de vida de los individuos. Es referenciable el paulatino aumento de la información por parte del Estado, invadiendo ámbitos hasta entonces ignorados de la vida privada de los ciudadanos, y almacenando toda una amplia gama de datos que, de ser cruzados a través de las técnicas de conexión de ficheros, pondrían al individuo en una situación de absoluta publicidad de ideas, sentimientos y opiniones, probablemente no deseada por él.

Este proceso de creación de registros y archivos públicos tiene su origen, como decimos, en la modernización del Estado, y alcanza, gracias al progreso cibernético, posibilidades hasta ahora insospechadas.

Con anterioridad a él, solo la Iglesia tenía una información más o menos completa de las circunstancias personales de sus fieles, a través de partidas de bautismo y certificados de matrimonio y de defunción, que proporcionaban los elementos necesarios para el conocimiento de la situación personal, civil, familiar, e incluso laboral de sus fieles.

Sin embargo, la burocratización creciente del Estado, y la expansión prácticamente indefinida de la Hacienda Pública, impulsada por la virtualidad efectiva de los postulados teóricos del Welfare State ha llevado a la puesta en marcha de un proceso de control que tuvo su inicio en nuestro país con la creación del Documento Nacional de Identidad, que albergaba ya desde su origen una pretensión no sólo identificativa sino controladora, y que sería el

primer paso para la creación de un código fiscal para el control de las actividades mercantiles y financieras de sociedades, compañías y asociaciones.

Este proceso ha cristalizado en nuestros días con la creación del Número de Identificación Fiscal –que guarda algunas similitudes evidentes con el código identificador único que se pretendió implantar en Francia a través del proyecto SAFARI– , que coloca al ciudadano en una situación de transparencia tributaria que provoca escalofríos al más contumaz defraudador.

Tras este proceso de acopio de información sobre los ciudadanos que podríamos calificar casi de biográfico, late no sólo la necesidad recaudatoria del Estado, sino también todo un bagaje teórico que requiere, para la virtualidad práctica del Estado Social, una información completa, detallada y exhaustiva sobre las circunstancias de los ciudadanos. El Estado Social ha erigido la actuación administrativa, a través de la prestación de servicios, en fin primordial de su actuación política, y con frecuencia se apelará al interés público como el principio rector de esta tensión dialéctica entre la privacidad y el derecho a la información. Queda patente, por lo tanto, que este proceso es fruto de una opción política definida, que apela al papel activo que el Estado ha de desempeñar en la promoción de los derechos y libertades de los ciudadanos.

Es obvio que todo ello contribuye a fortalecer los cauces operativos del Estado de Derecho, proveyendo a la administración de los medios necesarios para el ejercicio de su actividad, en la concreción de los principios redistributivos y socializadores que inspiran su orientación política.

Pero la encrucijada entre información, como derecho pasivo y activo a un tiempo –y por tanto, como garante de una participación real de los ciudadanos en el funcionamiento democrático del Estado–, e intimidad reclama un equilibrio entre el valor de lo privado y el interés legítimo de la colectividad. Y este apremio por establecer límites precisos ha de conllevar necesariamente una concreción de qué se entiende por intimidad si queremos vislumbrar un horizonte diáfano de libertad en la sociedad informatizada.

Es obvio que la entrada en vigor de la LORTAD supondrá la sumisión de estas conductas a los preceptos que en ella se contengan; pero el hecho en sí parece ser lo suficientemente grave y alertador como para suscitar una reflexión sobre el tema. En el fondo de la reflexión expuesta subyace el reconocimiento de una necesidad que proclamamos acuciante: la intimidad no puede quedar reducida a un ámbito mínimo, dejando la protección de ésta al arbitrio de lo que estimamos es una facultad excepcional, el habeas data.

La intimidad se configura como una categoría ampliamente diversa y heterogénea que aúna dentro de sí todo un complejo variado de situaciones que son susceptibles de defensa. Es conocida la distinción entre distintos niveles de la misma –lo secreto, lo íntimo y lo privado– a los que corresponderían distintos niveles de protección. Lo primero serían aquellos hechos o

noticias de la vida de la persona que deben permanecer ignorados; el espacio otorgado a lo íntimo hace referencia al ámbito de la vida personal y familiar que se desea quede libre de intromisiones; y, por último, la esfera de lo privado, comprende aquello que en una u otra medida afecta a las peculiaridades de la persona en singular (honor, nombre, imagen, etc). Y tenemos la sospecha de que el sistema de garantías que la LORTAD establece deja resquicios abiertos a la intranquilidad[1].

La posibilidad de equilibrar y ponderar es una necesidad de un ordenamiento constitucional que desea hacer efectiva la tutela de los valores que consagra, y por ello, el bien público debe actuar como criterio corrector de la privacidad en las situaciones en las que se requiera la publicidad de determinadas informaciones. Ello es así en supuestos conocidos tales como la posibilidad de vulnerar el secreto bancario, ya aludida, para hacer efectivo los principios recaudatorios de la Hacienda Pública. Pero entendemos que la extensión desmesurada de esta posibilidad en beneficio de agentes privados del mercado deja abierto una brecha peligrosa para el futuro de la libertad.

La contingencia histórica de la noción de intimidad no puede quedar al alcance de una interpretación restrictiva de un valor fundamental. La invasión de la intimidad puede revestirse en nuestros días bajo la apariencia de una función informadora de las operaciones financieras y de los activos patrimoniales reduciendo la defensa del espacio íntimo del sujeto a lo estrictamente ideológico –convicciones políticas, creencias religiosas o afiliación sindical, por ejemplo y a lo rigurosamente físico –estado de salud y vida sexual–.

Esta concepción restrictiva de la intimidad puede colocar al individuo al borde de un abismo insalvable y plantea la necesidad de recuperación de un ámbito íntimo más amplio. Bien es cierto que la actuación social del Estado requiere un caudal de información que sólo puede obtenerse a fuerza de hacer concesiones en el espacio íntimo del sujeto, y que éste, en virtud de ello, no puede entenderse como un valor protegible de manera absoluta.

Pero cabe el riesgo de que la invasión sea la norma y la prevención sea postergada por la labor indemnizatoria del perjuicio causado. Y esta posibilidad nos intranquiliza. El ejercicio de la autodeterminación informativa es un recurso necesario, pero no puede ser el único. Si hacemos concesiones en estas cuestiones acabaremos dejando abonado el terreno para una interpretación de nuestra convivencia democrática en clave orwelliana.

---

[1] Debo al Profesor PÉREZ LUÑO el haberme puesto sobre aviso de algunos de las deficiencias que posee el proyecto de Ley Orgánica reguladora del Tratamiento Automatizado de Datos Personales. En mayo del presente año tuve la ocasión de exponer una ponencia suya –la LORTAD. ¿Una ocasión perdida?– en el Encuentro sobre Informática y Derecho que anualmente organiza el Instituto de Informática Jurídica de la Universidad Pontificia de Comillas. A él me remito por ser sumamente esclarecedor sobre los méritos y deficiencias que aquejan al proyecto de ley en ciernes. Y a él también me adhiero en la medida en que comparto algunas de sus dudas acerca de la bondad del proyecto. En el fondo este trabajo no es otra cosa que la confesión de algunos de los temores que albergo con respecto a la LORTAD.

El habeas data no debe ser la norma, el mecanismo habitual a través del cual se concreta la protección efectiva del derecho a la intimidad, sino la excepción, el recurso esporádico ante las eventuales intromisiones ilegítimas que se puedan producir en la esfera privada del ciudadano.

El horizonte de la libertad en la sociedad tecnológica no debe quedar al arbitrio de una eventual protesta del ciudadano, sino que reclama un completo esquema de garantías que, a priori, eviten el ocasionamiento del perjuicio. De lo contrario pudiera ocurrir que el Estado social, que recaba para sí un papel activo en la promoción real de los derechos y libertades de los ciudadanos, acabe convirtiéndose en el verdugo de la libertad que tan fervientemente proclama.

BIBLIOGRAFIA

– BÉJAR, H., «El Ambito Intimo. Privacidad, individualismo y modernidad», *Alianza*, Madrid, 1988.

– CARMONA SALGADO, C., «Libertad de expresión e información y sus límites», *Edersa*, Madrid, 1991.

– FROSINI, V., «L'uomo artificiale. Etica e diritto nell'era planetaria», *Spirali,* Milano, 1986.

– LOSANO, M.G., «Il Diritto Pubblico dell'informatica», *Einaudi*, Torino, 1986.

– O'CALLAGHAN, X., «Libertad de expresión y sus límites: honor, intimidad e imagen», *Edersa*, Madrid, 1991.

– PÉREZ LUÑO, A.E., «Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las nuevas tecnologías de la información», *Fundesco*, Madrid, 1987.

«La Intimidad en la sociedad informatizada», en «Derechos Humanos, Estado de Derecho y Constitución», 3.ª ed, *Tecnos*, Madrid, 1990, pp. 345-357.

–«La LORTAD: ¿Una ocasión perdida?», ponencia presentada en los Encuentros sobre Informática y Derecho, Madrid, Mayo de 1992, (en prensa).

La presunción de inocencia y el deber de colaboración con la inspección de trabajo. Derecho de acceder a los archivos informáticos

JOSÉ JESÚS DE VAL ARNAL
Profesor Ayte. de Derecho del Trabajo y de la Seguridad Social.
Juez Suplente de lo Social
(ESPAÑA)

SUMARIO

I. INTRODUCCION
II. LA POTESTAD SANCIONADORA DE LA ADMINISTRACION, LA INSPECCION DEL TRABAJO Y LA PRESUNCION DE INOCENCIA
III. EL DEBER DE COLABORACION CON LA INSPECCION DE TRABAJO Y LA PRESUNCION DE INOCENCIA
1. La obstrucción a la labor inspectora
IV. LOS ARCHIVOS INFORMATIZADOS
V. PROPUESTAS DE REFORMAS NECESARIAS PARA LA INSPECCION DE TRABAJO
VI. CONCLUSIONES

I. INTRODUCCION

El tema se centra en una parte muy especial de la Intervención administrativa del Estado sobre las relaciones laborales: la Potestad Sancionadora por incumplimiento de la legislación social.

Como ya apuntó mi maestro [1] las técnicas sancionadoras en el orden social «se conectan al problema de la efectividad de las normas». «Para que el Derecho del Trabajo cumpla su función ordenadora de las relaciones laborales en una sociedad concreta, es preciso que sus normas se apliquen y proyecten sobre la realidad social».

La actividad inspectora se proyecta sobre los administrados y si bien existe una garantía máxima, –el procedimiento administrativo de imposición de sanciones–, en algunos momentos se puede pensar que la Administración parte en una situación de ventaja.

El trabajo que presento se centra en el «principio de presunción de inocencia» como principio inspirador de la Ley de Infracciones y sanciones en el Orden Social.

La presunción de veracidad de las actas levantadas por los Inspectores de Trabajo, el deber de colaboración o no obstrucción a la labor inspectora, la entrada en la empresa, chocan con el principio de presunción de inocencia.

Hoy se presenta un cambio tecnológico en la forma de archivar ciertos datos, que conlleva en los Inspectores la necesidad de acceder a los archivos informatizados. Y entonces surge la pregunta: ¿El deber de colaboración con la Inspección supone que se debe acceder a la inspección de archivos informatizados?

II. LA POTESTAD SANCIONADORA DE LA ADMINISTRACION, LA INSPECCION DEL TRABAJO Y LA PRESUNCION DE INOCENCIA

La Constitución Española en el art. 103, núm. 1, fija los fines de la Administración, y junto al art. 25, núm. 1 consagran la actividad limitadora de la Administración y el mantenimiento de un determinado orden, planteándose la potestad sancionadora de la Administración.

En el ámbito del Derecho del Trabajo y de la Seguridad Social, velar por el cumplimiento de la normativa de la legislación social es el motivo del nacimiento del cuerpo de la Inspección de Trabajo y de los Controladores laborales.

La Ley de Infracciones y sanciones en el Orden social de 1988 es el último código de sanciones en esta materia, que junto al Reglamento de la Inspección de trabajo que se regula en el Decreto 2121/71, de 23 de julio, el Reglamento 1860/75, de 10 de julio, que aprueba el procedimiento administrativo especial de imposición de sanciones por infracción de leyes sociales y para liquidación de cuotas de la Seguridad Social, la Ley 39/62, de 21 de

[1] RIVERO LAMAS, J.: «Sanciones por violación o incumplimiento de normas laborales». Informe al XII Congreso Internacional de Derecho del Trabajo y de la Seguridad Social. Tema I. Madrid. 1988, pág. 10.

julio, sobre ordenación de la Inspección de Trabajo, quedando como supletoria la Ley de Procedimiento Administrativo, de 17 de julio de 1958. Es el conjunto normativo para poder actuar y controlar el cumplimiento de la legislación social.

Frente a la defensa de la autonomía del Derecho Administrativo Sancionador se puede defender la aplicación de principios del Derecho Penal a éste. Uno de los principios básicos es el de la Presunción de inocencia.

En el Derecho Penal, se es inocente mientras no se demuestre lo contrario. El art. 24.2 de la Constitución proclama este principio. La presunción de certeza de las actas levantadas por un Inspector, que sólo alcanza a los hechos, y que no traslada la carga de la prueba, crea un problema por la desigualdad creada en el punto de partida de la actividad sancionadora. El procedimiento administrativo sancionador es una garantía del administrado, pero las actividades de la inspección son previas a la formulación del procedimiento administrativo. La denuncia por parte de la Inspección, –levantamiento de acta–, supone una determinada actuación que en el ámbito laboral suponen unas actuaciones muy concretas y que presentan ciertos roces con los derechos y garantías del administrado. El Proyecto de Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común presentado al Congreso recoge en el Título IX, el principio de presunción de inocencia entre los principios del Procedimiento sancionador:

III. EL DEBER DE COLABORACION CON LA INSPECCION DE TRABAJO Y LA PRESUNCION DE INOCENCIA

1.–La obstrucción a la labor inspectora.

El procedimiento administrativo sancionador, que debería ser la mayor garantía de los ciudadanos ante la actividad sancionatoria de la Administración, es un simple trámite porque la Administración a través de la actividad inspectora parte en una posición de ventaja. [2]

Como señala SUAY RINCÓN, el doble mecanismo que representa la presunción de veracidad de que gozan las actas levantadas por la Inspección por una parte, y la exigencia indiscriminada del deber de colaboración a los particulares (con acceso a todo tipo de documentación e incluso al propio domicilio profesional), por la otra, hacen que la Administración arranque en posición de ventaja y los particulares tengan las garantías debilitadas.

En el Derecho Administrativo Sancionador en el Orden Social el deber de colaboración no aparece como tal, sino en sentido negativo como «deber de no obstrucción». No se presenta como una obligación de hacer sino como de no hacer.

---

[2] SUAY RINCÓN, J.: «La discutible vigencia de los principios de imparcialidad y de contradicción». *RAP*, núm. 123, Septiembre-diciembre 1990, págs.

Art. 49 de la Ley de infracciones y sanciones en el Orden Social.

«Las acciones u omisiones que perturben, retrasen o impidan el ejercicio de las funciones que, en orden a la vigilancia del cumplimiento de las disposiciones legales, reglamentarias y convenios colectivos tienen encomendadas los Inspectores de Trabajo y Seguridad Social y los Controladores Laborales, serán constitutivas de obstrucción a la labor inspectora que se calificará como grave, excepto aquellos supuestos que impliquen un mero retraso en el cumplimiento de obligaciones de información, comunicación o comparecencia, que se calificarán como leves. Los supuestos de resistencia reiterada, coacción, amenaza, violencia, desacato o cualquier otra forma de presión ejercida sobre los Inspectores de Trabajo y Seguridad Social y los Controladores Laborales serán considerados como infracción muy grave.»

En el art. 14 del Decreto 2122/1971, de 23 de julio, por el que se aprueba el reglamento de la inspección de trabajo se define la obstrucción a la labor inspectora:

a) Negar la entrada al Inspector o su permanencia en el centro de trabajo visitado, aunque en él radique el domicilio del empresario o se trate de un taller familiar.

b) Impedir la entrada o la permanencia en cualquier lugar en donde se desarrollen algunas de las funciones cuya vigilancia tiene encomendada el Inspector de conformidad con el art. 2 del presente Reglamento.

c) Ofrecer resistencia activa o pasiva al examen de libros o documentos precisos para su actuación.

d) Ocultar datos y antecedentes sobre accidentes de trabajo y sus circunstancias, prestaciones de la Seguridad Social o cualquier materia de su competencia.

e) Ocultar personal o dificultar su declaración, en especial cuando se trate de cargos sindicales representativos de los trabajadores de la Empresa.

f) Presentar intencionadamente denuncias o declaraciones falsas.

g) Cualquier otra acción y omisión que perturbe, retrase o impida el ejercicio de la actuación inspectora.

Art. 4.º del Real Decreto 1667/1986, de 26 de mayo por el que se regulan los cometidos y atribuciones de los funcionarios en el desempeño de puestos de controladores laborales, dentro de la Inspección de Trabajo y Seguridad Social, y en este caso se considera obstrucción a la Inspección de Trabajo y Seguridad Social:

a) Prohibir la entrada o permanencia del Controlador en los establecimientos, centros de trabajo, locales y otros lugares donde se desarrollen actividades sujetas a su competencia, a salvo, siempre, la inviolabilidad de domicilio.

b) Ofrecer resistencia activa o pasiva al examen de los libros, registros o documentos que el Controlador juzgue necesario para su actuación.

c) Ocultar datos y antecedentes relativos a afiliación, altas y bajas de trabajadores asimilados, cotización y prestaciones de la Seguridad Social, e impedir que el personal al servicio del empleador facilite los datos o la información solicitada por los Controladores.

d) No presentar la documentación establecida en el ordenamiento jurídico que le haya sido requerida por el Controlador.

Esta es la posición en el Orden Social con respecto al deber de colaboración con la Inspección de Trabajo y que en otros ámbitos se distinguen por establecer un deber de colaboración. [3]

¿Pero qué documentos deben ser los presentados? ¿Dónde se regula «la documentación establecida por el Ordenamiento Jurídico»?

Serán los que el controlador «juzgue necesarios para su actuación» art. 4. b). R.D. 1667/86, de 26 de mayo, por el que se regulan los cometidos y atribuciones de los funcionarios en el desempeño de puestos de trabajo de Controladores Laborales, dentro de la Inspección de Trabajo y Seguridad Social.

De un estudio detallado de la Ley de Infracciones y Sanciones un empresario tiene los siguientes deberes en materia de DOCUMENTACION:

1.– Libro de Visitas de la Inspección de Trabajo.

2.– El calendario laboral.

3.– Recibos de salarios.

4.– Documento de control de la actividad laboral que se realiza.

5.– Contratos de trabajo por escrito.

6.– Documentación de los últimos 5 años que acredite el cumplimiento de las obligaciones en materia de afiliación, altas, bajas o variaciones que, en su caso, se produjeran, documentos de cotización, recibos justificativos del pago de salarios y del pago delegado de prestaciones.

7.– Libro de matrícula del personal.

8.– Obligaciones formales de las Mutuas Patronales relativas a diligencia, remisión y conservación de libros, documentos, boletines de cotización y relación nominal de trabajadores, así como boletines estadísticos. El Real Decreto 1509/1976, de 21 de Mayo, por el que se aprueba el Reglamento General sobre colaboración de las Mutuas Patronales de Accidentes de Trabajo en la Gestión de la Seguridad Social, en sus arts. 20, 21, 22, 23, 24, 25 y 26 establecen los libros que las Mutuas están obligadas a llevar al día,

[3] Art. 32 de la Ley15/89 de Defensa de la Competencia, art. 14 del R.D. 1945/83 sobre consumo, art. 111 de la Ley General Tributaria.

incluso la comunicación de los Presupuestos al Ministerio de Trabajo [4]. De otro lado está el control por la Intervención de la Seguridad Social.

9.– Empresas que colaboran voluntariamente en la Gestión: no llevar la documentación reglamentariamente exigida. Según la Orden de 25 de Noviembre de 1966 por la que se regula la colaboración de las empresas en la Gestión del Régimen General de la Seguridad Social, en el art. 8, letra e: «Llevar en su contabilidad una cuenta que recoja todas las operaciones relativas a la colaboración».

10.–Cooperativas. El art. 90 de la Ley 3/1987, de 2 de abril, enumera la documentación social:

Sin perjuicio de lo establecido en otras Leyes o disposiciones especiales, las Cooperativas llevarán en orden y al día los siguientes libros:

Toda esta documentación se puede exigir porque es una documentación que la Ley de Infracciones y Sanciones en el Orden Social, y el resto de la normativa en materia de los deberes documentales de sujetos (no todos los mencionados hasta ahora) empresarios.

En ningún momento en el Reglamento de la Inspección de Trabajo del año 1971 y en el Proyecto de Reglamento de la Ley de Infracciones y Sanciones se enumeran claramente los documentos:

art. 8º.8: La Inspección de trabajo podrá solicitar la colaboración de:

«8.– las empresas y trabajadores en general, que facilitarán los informes y documentación necesarios y oportunos».

Existe un deber general para todos los administrados que se recoge en la Ley de Procedimiento Administrativo, art. 27: [5]

«Los administrados están obligados a facilitar a la Administración informes, inspecciones y otros actos de investigación sólo en la forma y casos previstos en la Ley, o por disposiciones dictadas en virtud de las mismas».

Este artículo expresamente dice que se presentarán los informes en «la forma y casos previstos por la Ley». Habría que matizar a qué Ley se refiere. La intención del legislador es toda Ley que señale un deber documental o ha

---

[4] Libros: 20.1. Las Mutuas Patronales vendrán obligadas a llevar al día los siguientes libros:

20.1.1. Libro Registro de Empresas.

[5] En el Proyecto de Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (BOCG Congreso, Serie A, núm. 8-1, de 4 de marzo de 1992), en el art. 38 también se regula el deber de colaboración de los ciudadanos: Los ciudadanos están obligados a facilitar a la Administración informes, inspecciones y otros actos de investigación sólo en los casos previstos por la Ley.

En el art. 34 se defiende también al administrado para que no sea «obligado a presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate, o que ya se encuentren aportados a la Administración actuante.

de ser la Ley que reglamente la Inspección o en su caso el reglamento de inspección.

Para PÉREZ-ESPINOSA el examen de libros y documentos del empresario «está contraído a los documentos o libros que a efectos laborales esté obligado a tener el empresario: libro de matrícula, justificantes de altas y bajas, recibos de salarios, boletines de cotización...En relación a la posible utilización de los libros de contabilidad del empresario como medio de comprobar o investigar la existencia de infracciones laborales, el inspector de Trabajo deberá solicitar a la autoridad judicial que decrete su examen, a fin de dejar sin efecto el derecho al secreto de la contabilidad del empresario.» Cuestión que vuelve a reiterar al examinar los supuestos de obstrucción a la labor inspectora: «Este derecho de examen del inspector viene referido exclusivamente a los libros y documentos exigidos por las normas laborales y de Seguridad Social, quedando excluidos los libros de contabilidad sobre los que pesa las garantías contenidas en el Código de Comercio y en la LeCr». [6]

Desde luego no son iguales los poderes y facultades de la Administración y del Tribunal Penal a la hora de recabar y practicar pruebas. Mientras los Jueces y Tribunales cuentan con la obligatoriedad general de colaboración establecida en el art. 118 de la Constitución. Tan sólo se contempla la obligación de facilitar informes, inspecciones y otros actos de investigación (art. 27 LPA) y sin que, por otra parte, exista la previsión, con carácter general, de cuáles puedan ser las consecuencias del incumplimiento de tal deber [7]. Frente a esto está el derecho a no declarar y a no confesarse culpable. (GARBERI LLOBREGAT, SUAY RINCÓN).

Como ya adelantó GARBERI LLOBREGAT «la Constitución Española de 1978 no contempla el deber de los ciudadanos de colaborar con las Administraciones Públicas, salvo la de Justicia (art. 118 CE), con lo que se carece de base constitucional para exigir tales comportamientos» [8].

La Sentencia del Tribunal Constitucional de 26 de marzo de 1990 apunta que:

---

[6] PÉREZ-ESPINOSA SÁNCHEZ, F.: «Las infracciones laborales y la Inspección de Trabajo». *Ed. Montecorvo*, Madrid, 1977, págs. 162 y 169.

[7] En el anteproyecto de ley de régimen jurídico de las Administraciones Públicas –copia del MAP–, en el art. 38 se establece que los ciudadanos están obligados a facilitar a la Administración informes, inspecciones y otros actos de investigación sólo en los casos previstos por la Ley, y en la forma determinada por la misma o por disposiciones dictadas en virtud de una ley.

En el art. 34 se defiende también el administrado para que no sea «obligado a presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate, o que ya se encuentren aportados a la Administración actuante».

Igual al proyecto presentado al Congreso de Diputados.

[8] GARBERI LLOBREGAT, J.: «Presunción de inocencia "versus" deber de colaboración cívica con la Administración sancionadora», PJ núm. 14, pág. 119. Se defiende la reforma del art. 278.2 del Código de circulación para poder exigir la colaboración con la Administración por parte del titular del vehículo.

«no existe un derecho absoluto e incondicionado a la preserva de los datos del contribuyente con relevancia fiscal y esgrimible frente a la Administración Tributaria. Tal pretendido derecho haría virtualmente imposible la labor de comprobación de la veracidad de las declaraciones de los contribuyentes a la Hacienda Pública y, en consecuencia dejaría desprovisto de toda garantía y eficacia el deber tributario que el art. 31.1 de la Constitución consagra, lo que impediría una distribución equitativa al sostenimiento de los gastos públicos en cuanto bien constitucionalmente protegido... Cuando el contribuyente aporta o exhibe los documentos contables pertinentes no está haciendo una manifestación de voluntad ni emite una declaración que exteriorice un contenido admitiendo su culpabilidad.» [9]

Si bien en el ámbito tributario las normas regulan claramente los deberes documentales, se puede presentar como contrario a la Ley de Enjuiciamiento Criminal (art. 391.3) el que el sujeto tributario la realización de una conducta que puede acabar en los tribunales penales, porque a pesar de ser una actividad inspectora con carácter administrativo puede determinar una causa de imputación penal. El Derecho a no declarar contra sí mismo y a no declarar son derechos que se manifiestan en el derecho a la presunción de inocencia.

¿Qué principios informadores de la Ley de Infracciones y Sanciones se ven forzados por este deber de no obstrucción o deber de colaboración?

En primer lugar se matiza el principio de contradicción, principio inmerso en el procedimiento; en segundo lugar se infringe el principio de presunción de inocencia, no sólo a efectos sancionatorios administrativos, sino a efectos de sanción penal.

Para el Tribunal Constitucional la cobertura de todas las actividades inspectoras no podrán juzgarse inconstitucionales por presunta vulneración del derecho a no confesarse culpable o en aplicación del principio de presunción de inocencia, porque, como ha tenido oportunidad de señalar en la STCO 76/1990, de 26 de abril, FD 10 recaída en relación con el art. 83.1.f) de la Ley General Tributaria que sanciona «la falta de aportación de pruebas y documentos contables o la negativa a su exhibición, existe un deber de aportar los datos que puedan ayudar a la investigación, y la exhibición de tales datos no puede considerarse como una colaboración equiparable a la declara-

[9] En el anteproyecto de ley de régimen jurídico de las Administraciones Públicas, –copia del MAP–, en el art. 46 se intenta impulsar el empleo y la aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de la actividad y ejercicio de sus competencias, con las limitaciones que la utilización de estos medios establecen la Constitución y las Leyes, que cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de las técnicas y medios electrónicos, informáticos o telemáticos con respecto de las garantías y requisitos previstos en cada procedimiento.

En todo caso los procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y regular ejercicio del órgano que ejerce la competencia.

ción comprendida en el ámbito de los derechos proclamados en los arts. 17,3 y 24.2 de la Constitución.

Pero no hay que olvidar en ningún momento que «en los supuestos en que las infracciones pudieran ser constitutivas de delito, la Administración pasará el tanto de culpa al órgano judicial competente o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador». [10]

IV. LOS ARCHIVOS INFORMATIZADOS

Como hemos podido observar en la legislación sobre la actividad sancionadora en el Orden Social, no se menciona el archivo informatizado como supuesto de hecho, del deber de colaboración, para proceder a obtener información por parte de la Inspección.

Ni siquiera sobre la posibilidad de sacar muestras, es decir copia de un disco duro o discos flexibles. [11]

Sólo conocemos hasta ahora una resolución de un tribunal sobre el tema de archivos informatizados y uno de los procedimientos de obtención de información que se desprenden del art. 111 de la Ley General Tributaria es el requerimiento individualizado de la Administración con los plazos y requisitos que reglamentariamente se determinen.

El Tribunal Económico Administrativo Central en Pleno, en Resolución de 28 de Febrero de 1990, estima que el requerimiento de información a terceros se ajusta a derecho, y por tanto la entidad aseguradora ha de suministrar los datos requeridos. Se trata de un deber de colaboración a terceros, pero que demuestra el interés de que se suministre un archivo informatizado, por parte de la Inspección del Ministerio de Hacienda. La forma en que se solicitó: Soporte magnético ajustado a las siguientes características técnicas: Cintas:9 pistas, 1600 BPI, Código EBCDIC, sin etiquetas y con marca TM de fin de cinta. Factor de Bloqueo 10, Diskette de 3 1/2 pulgadas, doble densidad, (720 K), de 5 1/4, doble cara, doble densidad, (360K); doble cara, alta densidad (1,2 MB), So.: MSDOS.

La evolución normativa no ha impuesto salvo en un caso y para supuesto de obligación de suministrar información con carácter general, la obligación de colaborar con la Administración Tributaria suministrando información en soporte informatizado y nunca para los requerimientos individualizados.

---

[10] Art. 3.º1 de la Ley de Infracciones y sanciones en el Orden Social.

[11] El art. 22 del Reglamento de la Inspección de Trabajo establece los medios autorizados para realizar su función y entre ellos se establece en la letra h):

realizar mediciones y tomar o sacar muestras de sustancias y materiales utilizados o manipulados en el centro de trabajo, como asimismo para obtener fotografías y levantar croquis y planos, previa notificación al empresario o su representante.

Estas operaciones las podrá realizar el Inspector directamente o por persona por él designada y a su presencia.

Así la OM de 3 de diciembre de 1979 autoriza el cumplimiento de las obligaciones tributarias mediante soportes legibles por ordenador, la OM 11 de diciembre 1979, IRPF e IS, regula determinadas obligaciones de información y en su número III cuando se habla de «modelos», dice en el ap. 3, «cuando el M. de Hacienda lo autorice los obligados a presentar resúmenes y relaciones podrán sustituir los impresos oficiales por soportes magnéticos directamente legibles por ordenador, con el formato de registro que, en cada caso, se apruebe por la DGT.; la Resolución de 20 de abril de 1981 DGT, aprueba normas y diseños para sustituir las hojas interiores de modelos 190 y 191 por soportes magnéticos legibles directamente por ordenador, y en su art. 1 se hace referencia al carácter opcional de esta forma de cumplir con el deber de información por la persona física o jurídica obligada, en términos parecidos y siempre con carácter opcional de esta forma de cumplir con el deber de información por la persona física o jurídica obligada; en términos parecidos y siempre con carácter facultativo se expresa la R. 10 de noviembre 1981 DG Inspección Tributaria en relación con el modelo 192; la R 4 de noviembre de 1985 de la citada DG aprueba los modelos de declaración de retenciones directas e indirectas a cuenta y diseños físicos y lógicos para sustituirlos por soportes magnéticos, señalando en la Instrucción Tercera, ap. 2 el carácter opcional para presentar las declaraciones en una u otra forma, también en la OM 11 de febrero de 1986 y en relación con los modelos 193, 194, 196 y 198 se utiliza la expresión optase aplicable al obligado tributario, finalmente el RD 2529/1986 de 5 de diciembre regula de la declaración o relación anual que deben presentar los empresarios o profesionales acerca de sus operaciones con terceros, y la OM 2 mar. 1987 dictada en su desarrollo, por la que se aprueban las condiciones y diseño de los soportes magnéticos válidos para sustituir las hojas interiores del modelo de la declaración anual de operaciones, donde se dice que esta forma de presentación es obligatoria cuando el número de personas o Entidades relacionadas en la declaración exceda de 500 y en el declarante concurran otras condiciones las cuales no es preciso transcribir porque, aun cuando en el supuesto que nos ocupa la relación a aportar por la reclamante comprendiera más de 500 talleres de reparación de vehículos la obligación de suministrar esta información no ha venido motivada por una disposición de carácter general sino por un requerimiento individualizado de la Administración, en resumen no existe disposición alguna que obligue a aportar información en soporte magnético cuando media requerimiento individualizado para aportar datos y solamente cuando estos deben suministrarse con carácter general se concede la opción al obligado para o bien cumplimentar el modelo oficial o bien sustituir las hojas interiores por soportes magnéticos, con la excepción de obligado cumplimiento ya mencionada.

El principio de Legalidad y Tipicidad –propios del Derecho Administrativo sancionador–, tienen su manifestación en este tema, y tanto en el Ordena-

miento Tributario como Social la falta de tipificación como documentación a mostrar a la Inspección de los archivos informatizados, deja a estos fuera del control de la Inspección.

V. PROPUESTAS DE REFORMAS NECESARIAS PARA LA INSPECCION DE TRABAJO

En el Proyecto de Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, (BOCG, Congreso, Serie A, núm. 8-1, de 4 de marzo de 1992), en el art. 44 se hace una declaración de principios sobre la incorporación de medios técnicos. Con ello se va hacia una progresiva utilización de medios por parte de la Administración lo que incide posteriormente en los administrados para que éstos posteriormente utilicen éstos y la Inspección sea sobre soporte magnético.

Por todo esto es necesario una Reforma de la Ley de Infracciones en el Orden Social, para poder acceder a los archivos informatizados y sacar copias.

En el terreno práctico de formación es precisa una reforma del temario de oposición del Cuerpo de Inspectores y controladores laborales que incluya unas lecciones sobre informática (nivel básico), así como posteriormente en las prácticas realizar pruebas con mini-ordenadores y ordenadores personales.

A ello hay que unir que el tema no sólo es necesario por el control de cierta documentación, sino por el tema de Seguridad e Higiene en centros de procesos de datos en que el control de tiempo de trabajo y de la propia labor desempeñada por el trabajador, se hace por la propia herramienta (ordenador) y sin conocimiento de acceso a éste es imposible saber el cumplimiento de tiempos ante la pantalla.

VI. CONCLUSIONES

1.– Sólo en los casos de colaboración voluntaria del administrado ante la Inspección de Trabajo y Seguridad Social se puede acceder a los archivos informatizados para localizar información necesaria para la actividad inspectora.

2.– En el supuesto de que el Inspector o controlador laboral intente acceder a documentación que esté en soporte magnético la aplicación del principio de tipicidad, del principio de legalidad y el de presunción de inocencia no obligan al administrado a informar sobre datos en este tipo de soporte y existen serias dudas en el procedimiento administrativo sancionador sobre la diligencias preliminares de la Inspección a la hora de solicitar la colaboración del administrado ya que los hechos descubiertos por el inspector o el controlador laboral pueden acabar en responsabilidad penal.

3.– Es necesaria una reforma del procedimiento administrativo sancionador general y del procedimiento en materia Social para posibilitar el acceso de los Inspectores a los archivos informatizados a la vez que se garanticen los derechos del administrado en un procedimiento que tiene como primera fase las diligencias preliminares y no apertura de expediente.

Ahora que se está debatiendo en las Cortes Españolas el proyecto de Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo es el momento oportuno para garantizar las reformas necesarias.

Administración pública, informática y ciudadano: perspectiva general

MARCOS MATIAS FERNANDO PABLO
Doctor en Derecho. Departamento de Derecho Público de la Universidad de Salamanca
(ESPAÑA)

SUMARIO

I. INTRODUCCION
II. DOCUMENTOS, REGISTROS Y PROCEDIMIENTOS ADMINISTRATIVOS EN SOPORTE INFORMATICO
2.1.–La validez de los documentos informáticos.
2.2.–Registros y procedimientos administrativos en soporte informático.
III. LA POSICION DEL ADMINISTRADO: UTILIZACION DE SOPORTE INFORMATICO Y ACCESO A DOCUMENTOS ADMINISTRATIVOS

I. INTRODUCCION

La poupe informatique [1] recibe, cada vez más, cuantiosos fondos públicos y atenciones presupuestarias por parte de nuestras Administraciones públicas, empeñadas, muchas veces, según parece, en hacer informáticamente más difícil al ciudadano todo aquello que requiere el empleo de

[1] Vid BRAIBANT: «L'informatique dans l'administratión», *Rev. Intern. Scien. Adminis.* 1969. pág.341

tiempo humano de atención administrativa, sin que, hasta el presente, se haya observado entre nosotros, una preocupación normativa por clarificar las posiciones jurídicas de Administración y ciudadano ante la alteración de los modos y formas habituales de relación que aquella ocasiona.

Ello se ha traducido, a falta de legislación general y ante la inadecuación de la vigente Ley de Procedimiento Administrativo, en que los modos operativos y las caracteristicas de los soportes informáticos han sido disciplinados por normas administrativas de ínfimo rango y de caracter prevalentemente parcial e interno, sin que por ello dejasen de tener importantes repercusiones sobre los administrados. Sirvan de ejemplo la Circular de 13 de febrero de 1976 (que creó el concepto de «Dato de interes opolicial» y especificó su régimen jurídico), junto con la conocida Orden Ministerial de 30 de junio de 1982 que reguló el acceso a las bases de datos de caracter tributario de la Administración Pública, o la Resolución 1/92 de la Dirección General de la Agencia Estatal de la Administración Tributaria por la que se establecen determinadas características del sistema informático que ha de soportar el procedimiento de devolución de ingresos tributarios que regula, y entre ellas, la posibilidad de un cruce de datos entre distintos bancos, antes de determinar el importe de una devolución, realizando así una compensación electrónica que puede resultar muy poco clara para el administrado.

El examen general del fenómeno[2] sólo ha sido abordado, recientemente, entre nosotros, por el Proyecto de LORTAD desde una perspectiva habitual de **«protección de datos»,** y por el **Proyecto de Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común** (en adelante, LRJAPC)[3] en lo que se refiere a las relaciones entre la Administración y los ciudadanos, ocupándose, este último proyecto, no sólo del aspecto de garantía, sino también de las aplicaciones de la informática en el procedimiento administrativo, en los términos que pasan a describirse problemáticamente, y que abarcan tanto el empleo de medios informáticos por la Administracion (el régimen de los documentos, registros y procedimientos administrativos en soporte informático) como la posición de los particulares frente a los mismos (acceso a los documentos y registros en soporte informático, notificaciones, recursos frente a medios de gestión informática y sus resultados...).

---

[2] A propósito del cual se ha señalado que puede dar lugar a una «intensificación de las inclinaciones hacia un perfeccionismo burocrático, una reducción de las posibilidades de participación de los ciudadanos y una ampliación del control por parte de la Administración». Vid. LÓPEZ BUSTOS y LÓPEZ SIDRO JIMÉNEZ: «Informática, administración y derecho a la intimidad», en RIVERO. A. Ed. Introducción a la informática jurídica. *Fundesco*, Madrid 1986.

[3] El proyecto fue publicado en el BOCG del 4 de marzo de 1992, serie A, núm. 82. Utilizaremos también, en la exposición que sigue el texto del Anteproyecto de fecha 18 de julio de 1991.

II. DOCUMENTOS, REGISTROS Y PROCEDIMIENTOS ADMINISTRATIVOS EN SOPORTE INFORMATICO

2.1. La validez de los documentos informáticos.

El citado Proyecto de LRJAPC se preocupa de indicar que si bien la Ley de Procedimiento Administrativo ya pretendió modernizar la arcaica Administración española propugnando la «racionalización de los trabajos burocráticos y el empleo de máquinas adecuadas», tan limitado planteamiento imposibilitó que «la informatización haya tenido hasta ahora incidencia sustantiva en el procedimiento administrativo», limitándose la tecnificación operativa de las Administraciónes Públicas «al funcionamiento interno, sin correspondencia relevante con la producción jurídica de su actividad relacionada con los administrados» .

Tal resultado se debe, según la Exposición de Motivos del Proyecto que viene citándose, en la falta de reconocimiento formal de la validez de documentos y comunicaciones emitidas por via informática. De aquí que sea éste el primer punto de interés del Proyecto de Ley al reconocerse expresamente que «los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas o los que éstos emitan como copias de originales almacenados por los mismos medios, gozarán de la validez y eficacia de documento original...» (art. 44) siempre que se cumpla el triple requisito de que a) se garantice su conservación o integridad, b) se garantice la recepción por el interesado (cuando deba ser notificado) y c) quede a salvo el cumplimiento de los requisitos y de las garantías exigidas por el ordenamiento jurídico.

De estos requisitos es el tercero el que puede presentar una mayor problemática, pues el primero es un requisito común a todo documento como soporte de una información y el segundo ya venía exigido por la vigente LPA al admitir la notificación por medios que en todo caso deberían **dejar constancia de la recepción por el interesado.**[4]

En la declaración general del Proyecto de Ley de que los documentos emitidos por medios electrónicos por las Administraciones Públicas tendrán no sólo **validez,** sino también eficacia (art. 44-5) se implican ambas categorías, pues si la validez se determina por los requisitos aludidos, la **eficacia** dependerá de que quede garantizada la **recepción por el interesado,** expresión en la que parece que deben incluirse también los aspectos apuntados por la LPA, debiendo garantizar el documento emitido por medios informáticos, por tanto, el contenido, la identidad y la fecha de

[4] Art. 80: «Las notificaciones se realizarán mediante oficio, carta, telegrama o cualquier otro medio que permita tener constancia de la recepción, de la fecha y de la identidad del acto notificado».

la recepción, aspectos que el propio Proyecto de Ley (art. 57) exige para cualquier medio de notificación.

El requisito de que los documentos emitidos por medios informáticos, electrónicos o telemáticos cualquiera que sea su soporte (admitiéndose, por tanto, también el soporte informático) **garanticen el cumplimiento de las garantías y requisitos exigidos** por el ordenamiento jurídico (art. 44-5 in fine del Proyecto de LRJAPC) es el más problemático, dado que el empleo de modos informáticos se traduce, sustancialmente en alteraciones de la posición del particular que comienzan con la **rigidez del modelo impreso de captura de datos** relevantes para el sistema, y continúan con la dificultad de hacer valer los derechos del interesado en un procedimiento y finalizan en la alteración de las garantías derivadas de los **requisitos de forma de la resolución.**

Por lo que se refiere al primer punto, el Proyecto de LRJAPC se ha cuidado de indicar que si bien «Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias» (art. 44-1) tales medios se someterán a los límites señalados por la Constitución y las Leyes, añadiendo más específicamente el art. 68-4 que «Las Administraciones Públicas deberán establecer modelos y sistemas normalizados de solicitudes cuando se trate de procedimientos que impliquen la resolución de numerosos expedientes», si bien (y el correctivo respecto de los impresos de captura de datos puede ser bastante importante cara al administrado que no encuentra lugar en las casillas del impreso para hacer patente su singular situación o los datos que especifican su posición) «Los solicitantes podrán acompañar a éstas **los elementos adicionales** que estimen convenientes **para precisar o completar los datos del modelo,** los cuales **deberán ser admitidos y tenidos en cuenta** por el órgano al que se dirijan». Si con relación al modelo-solicitud inicial se ha establecido aquella regla, no es innecesario advertir que el principio que la inspira (a fin de cuentas, el principio antiformalista, en abierta pugna con la necesaria formalización de los documentos de captura de datos) es de aplicación también a cualquier otro trámite posterior (por ejemplo, las alegaciones del interesado o aportación posterior de nuevos datos o modificación sobrevenida de los iniciales) en el que, igualmente, se haya de utilizar los modelos previstos: la Administración estará obligada a admitir los elementos adicionales ofrecidos por el interesado junto a tales modelos normalizados.

Por lo que se refiere a la alteración de los requisitos de forma de los actos administrativos contenidos en documentos generados por medios informáticos es fundamental evitar que el ciudadano se enfrente «a los resultados brutos de los cálculos del ordenador[5]» afirmando, por el contra-

[5] Vid. BRAIBANT: «L'informatique...» cit. pág. 341

rio, que en ningún caso, la intervención de medios informáticos puede eludir la exigencia de **motivación expresa de los actos** o decisiones administrativas.

Este riesgo es bien patente, como lo prueba la temática de las «liquidaciones tributarias paralelas[6]», uno de cuyos patentes defectos jurídicos es la reducida o escasa motivación con la consiguiente falta de información y justificación que puede no respetar lo previsto en el art. 43 de la LPA y el art. 121-2 de la Ley General Tributaria, según los cuales deben ser motivados con sucinta referencia a hechos y fundamentos jurídicos, los actos que limiten derechos, debiendo los actos de comprobación que determinen un aumento de base tributaria sobre el resultante de las declaraciones del sujeto pasivo, contener igualmente, la debida motivación.

Debería por ello establecerse, junto con la posibilidad de dictar documentos que contienen actos administrativos sujetos al deber de motivación (que inequívocamente debe contener elementos singulares, de no fácil carácter algorítmico) la necesidad de una **motivación específica** e individualizada, actuable a petición del interesado, y suministrada al margen del sistema de gestión.

2.2.–Registros y procedimientos administrativos en soporte informático.

Con relación a los registros en soporte informático, el Proyecto de Ley se muestra en exceso rígido[7] estableciendo que las Administraciones Públicas **deberán instalar en soporte informático** los registros generales (art. 37-3), olvidando la existencia de numerosas entidades locales, de escasos recursos, y escasas necesidades de gestión, en los que no se ve la utilidad de registros informáticos

Por otra parte, los registros informáticos no son en absoluto una novedad y éste parece haber sido un campo de fácil introducción informática. Las especificaciones del Proyecto de Ley, por ello, responden a exigencias prácticas satisfactoriamente cumplidas por programas al uso. Así, cuando se exige que el sistema garantice la constancia, en cada asiento, de un número, epígrafe expresivo de su naturaleza, fecha de entrada, fecha y hora de su presentación, identificación del interesado y persona u órgano al que se envía, así como, en su caso (es decir, cuando sea exigido por una norma) referencia al contenido (apartándose en este

[6] Vid. por todos, CLAVIJO HERNÁNDEZ; «La liquidación: Liquidaciones provisionales y definitivas» *Actualidad Administrativa*, 14 y 15, 1990. CAZORLA PRIETO: «Las llamadas liquidaciones paralelas en el IRPF», *CISS*, Bilbao 1988.

[7] La Disposición Adicional Segunda del Proyecto establece: «La incorporación a soporte informático de los registros a que se refiere el art. 37 de la Ley será efectiva en la forma y plazos que determinen el Gobierno, los órganos de gobierno de las Comunidades Autónomas y la Entidades que integran la Administración Local, en función del grado de desarrollo de los medios técnicos de que dispongan».

punto de la LPA vigente que señala que «no deberá consignarse en el registro extracto alguno del contenido») no se está sino recogiendo la experiencia ya asentada, por ejemplo en el proyecto INFORIUS a propósito de los registros de la oficina judicial.[8]

El proyecto de Ley exige al sistema que soporte el registro que sea susceptible de integrar informáticamente en el registro general las anotaciones de los restantes registros del organo (art. 37-3) y mediante convenios prevé la posibilidad de intercomunicación con los registros compatibles informáticamente de otras Administraciones (art. 37-4).

Por lo que se refiere a los procedimientos en soporte informático, la referencia fundamental del Proyecto de Ley es el art. 44.3 según el cual, **«Los procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y el regular ejercicio de la competencia por el órgano que la ejerce»,** regla que responde a la lógica exigencia de legalidad en el ejercicio de la competencia, pero que no aclara demasiado cómo reaccionar ante un soporte informático que no garantiza la legalidad del ejercicio de la competencia, sino que da lugar a un ejercicio irregular de la misma (por ejemplo, omitiendo el trámite de alegaciones, o haciendo imposible que éstas puedan ser tenidas en cuenta al resolver por el órgano competente, vulnerando así lo establecido en el art. 83 de la LPA según el cual los interesados podrán en cualquier momento aducir alegaciones que serán tenidas en cuenta por el órgano competente al redactar la propuesta de resolución).

Ante un sistema informático que soporta un procedimiento administrativo, pero conduce a resultados semejantes, cabe preguntarse si el interesado podrá únicamente reaccionar contra la resolución, contra el acto final, alegando tales defectos, o por el contrario, una vez constatado que es el sistema el que no garantiza el regular ejercicio de la competencia, podrá plantearse algun tipo de remedio frente al mismo.

Desde una amplia perspectiva histórica se hace fácilmente demostrable cómo la normativa actual de procedimiento no es, en su conjunto, más que el resultado de la juridificación (es decir, del reconocimiento del carácter vinculante, con posible alegación por parte de terceros) progresiva de normas internas de la Administración reguladoras de actividad material e interna. Desde este punto de vista, parece posible admitir que esa progresiva juridificación debe alcanzar también hoy en día, a la **actividad material que soporta informáticamente, un procedimiento administrativo,** que es la calificación que cabe otorgar, segun creemos, a la ejecución del programa de gestión.

---

[8] Vid. sobre el mismo, en los aspectos registrales, la exposición de GIMENO AMIGUET: «La informática en la Administración de Justicia» en RIVERO Ed. Introducción a la informática. *Fundesco*, Madrid 1986.

Por eso, la **juridificación** debe alcanzar a controlar no sólo el resultado del procedimiento en soporte informático, sino a este mismo soporte, producto informático que debe contrastarse con el ordenamiento jurídico, dejando así de ser pura actividad interna, no relevante ad extra.

Pero en ese contraste, nuestro ordenamiento sólo conoce las categorías de **acto administrativo y disposición general,** (vid. art. 1-1 de la Ley de la Jurisdicción Contencioso-Administrativa) por lo que debe precisarse la naturaleza del programa de gestión, cuya ejecución permite tramitar un procedimiento administrativo en soporte informático.

El Proyecto de Ley no es ajeno a estas ideas. En primer lugar, intenta **juridificar el programa de gestión,** (respondiendo a las ideas antes descritas, de una actividad puramente interna que adquiere progresivamente, por obra de la normas de procedimiento relevancia jurídica ad extra), estableciendo, en general, que «**Los programas** y aplicaciones electrónicos **informáticos** y telemáticos que hayan de ser utilizados por las Administraciones Públicas «para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente quien difundirá públicamente sus caracteristicas» (art. 44-4).

El precepto plantea la cuestión, una vez admitido el posible recurso frente a tal **aprobación** (por ejemplo, por qué el programa aprobado omite la solicitud y recepción **de un informe preceptivo,** o no contempla la función **estimación de recursos** etc etc...) plantea la cuestión decíamos, de si el recurso debe plantearse frente a un **acto** frente a un **reglamento.**

Ello no es más que la traducción de la cuestión acerca de la naturaleza jurídica del programa. El Proyecto no aporta claves decisivas, y siendo en el fondo una cuestión de derecho positivo el decidir si el acto de aprobación se considera reglamentario o no, parece que «la difusión de las características» que se exige, debe equiparase a una publicación normativa, considerándose, por tanto, las características del programa (y por tanto, éste mismo) como norma reglamentaria. A ello apunta, por lo demás, una cartacterística esencial del programa de gestión como producto informático: la susceptibilidad de **aplicación reiterada sin consunción,** dato en el que, evidentemente, coincide con la norma reglamentaria.

Conceptuado el programa como norma reglamentaria, el recurso posible frente al acto de aprobación del mismo (art. 1 Ley de la Jurisdicción) debe realizarse de acuerdo con los distintos recusos frente a reglamentos que contempla nuestro ordenamiento, incluyendo, por tanto, la **posibilidad de recurso indirecto frente a aquél, mediante la impugnación de actos singulares de aplicación-ejecución,** o bien el recurso directo frente al mismo, equiparando a efectos de plazo, la publicación a la difusión pública de las características del programa, lo cual **no obliga, por cierto, a publicar la totalidad del programa,** sino especificar sus caracteres, desde

el punto de vista del «regular ejercicio de la competencia del órgano» (art. 44-3 Proyecto de LRJAPC).

III. LA POSICION DEL ADMINISTRADO: UTILIZACION DE SOPORTE INFORMATICO Y ACCESO A DOCUMENTOS ADMINISTRATIVOS

A fin de que los particulares puedan acceder al registro general de cada órgano administrativo mediante medios informáticos, se ha previsto que las Administraciones **deberán hacer públicos sus sistemas de acceso y comunicación así como los horarios de funcionamiento** (art. 37-7), al tiempo que se sienta el principio general de que los ciudadanos podrán relacionarse con las Administraciones **para ejercer sus derechos** a través de técnicas informáticas o telemáticas, **con respeto de las garantías y requisitos previstos en cada procedimiento.**

Ello posibilita que pueda accederse al Registro de entrada, mediante el cumplimiento de los requitos legalmente señalados, a través de instrumentos y medios informáticos y telemáticos, incluso sin intermedio de documento escrito en soporte de papel, técnica ésta que el conjunto de preceptos citados apunta a legalizar, como ratifica el art. 37 al exigir el registro no sólo de escritos sino también de «comunicaciones», o preveer que también éstas deben ser registradas por el sistema (art. 37-3), sin que a tal expresión pueda dársele el sentido restringido que tenía en la LPA en la que alude a documento escrito: vid. art. 65: registro de **todo escrito comunicación u oficio,** art. 65-3: documento, 65-4: escrito comunicación u oficio; art. 66: escritos o instancias...

En su caso, de admitirse prácticamente estas técnicas (y para ello la Administración debe publicar sus sistemas y horarios, de acceso art. 37-7) podría plantearse la duda, ante el posible carácter no instantáneo de la anotación en el registro general de la comunicación, de los datos temporales que deberían tomarse como referencia, cuestión que la vigente LPA resuelve indicando que «se entenderá que los escritos han tenido entrada en el órgano administrativo en la fecha en la que fueron entregados...».

De pretender una norma semejante respecto de la presentación de documentos generados y enviados por medios teleinformáticos y respecto de «comunicaciones» o mensajes no documentados en papel (comunicaciones que contengan, por ejemplo, la instancia inicial de un procedimiento, la interposición de un recurso o la formulación de alegaciones o aportación de datos) habrá que precisar que debe tomarse en consideración sólo su registro y recepción, a cuyo fin, los sistemas en uso deben **permitir acreditar al interesado tanto la presentación como la fecha y hora de la recepción, registro e identidad de la comunicación.**

Queda, por último, examinar el aspecto relativo al acceso de los ciudadanos (art. 105 C.E.) a los documentos y registros administrativos, supuesto en el que puede darse un conflicto entre la legislación general que establece el Proyecto al regular entre otros el derecho de los administrados «al acceso a los registros y Archivos de las Administraciones Públicas», derecho que, permite a los ciudadanos acceder «a los **registros** y a los **documentos** que formando parte de un expediente obren en los archivos administrativos **cualquiera que sea** la forma de expresión, gráfica sonora en imagen o **el tipo de soporte material en que figuren** siempre que tales expedientes correspondan a procedimientos terminados...» (art. 36-1 Proyecto de LRJAPC).

El acceso a tales documentos, puede conllevar, por tanto el derecho a acceder a archivos informatizados que plantean el problema de la protección de datos, perspectiva en la que convergen la futura legislación de protección de datos y el derecho de acceso a los archivos y registros administrativos, con el riesgo de dar lugar a normativas no homogéneas.

El Proyecto de LRJAPC establece que «el acceso a los documentos que contengan **datos referentes a la intimidad** de las personas estará reservado a éstas», otorgando a la persona titular una modalidad de el derecho de **habeas data,** señalando que el titular «en el supuesto de observar que tales datos figuran incompletos o inexactos podrá exigir sean rectificados o completados», derecho que no podrá ejercerse cuando tales datos figuren en expedientes caducados de los que no pueda derivarse efecto sustantivo alguno. (art. 36-2). Este precepto (de evidente signo protector frente a los **datos que afecten a la intimidad** y figuren en archivos administrativos, en soporte informático o convencional) puede plantear la duda interpretativa de si su ambito se extiende a cualquier archivo, o, por el contrario, los archivos en soporte informático deben regirse íntegramente (tanto en el acceso por parte de **ciudanos no interesados** en el procedimiento original, como en el régimen de consulta y ejercicio del habeas data) por la futura Ley de Protección de Datos, que, en desarrollo del art. 18-4 de la Constitución deberá tener carácter de Ley Orgánica.

Una interpretación sistemática que pretenda salvar las regulaciones de los dos proyectos de ley en curso (el de Ley de Proteción de Datos y el de Procedimiento Administrativo Comun) debe partir del ámbito específico de la primera, de manera que la protección frente a las aplicaciones informáticas debe encontrar allí su regulación total, tanto si es la Administración quien elabora y almacena datos personales, como si no.

Por tanto, la regulación del derecho de acceso a Archivos y Registros administrativos que se establezca en desarrollo del art. 105 C.E., por la regulación del procedimiento administrativo común, **no puede afectar a los datos de los archivos y registros en soporte informático,** al menos

cuando los documentos contengan datos referentes a la intimidad, respecto de los cuales debe aplicarse en su integridad la legislación (orgánica) de protección de datos.

Sólo a falta de norma expresa en ésta, será aplicable lo previsto en la futura Ley de Procedimiento Administrativo Común, y siempre que no esté en juego la intimidad de las personas, pues la protección de ésta frente a los archivos y registros administrativos informatizados debe tener rango de Ley Orgánica. (art. 18-4 y 81 C.E.).

El Proyecto de Ley de LRJAPC establece también que el acceso a documentos (en soporte informático o no) de carácter nominativo **que no incluyan datos referentes a la intimidad de las personas,** está abierto (salvo que se trate de expedientes sancionadores) tanto a los titulares como a **terceros que acrediten un interés legítimo y directo.**

La diferencia de sujetos titulares del derecho de acceso, según los datos afecten o no a la intimidad, plantea el problema de cuales son tales datos, que, en nuestra opinión, debe corresponder, en principio a los llamados **«datos sensibles»,** es decir los referentes a la ideología, religión, creencias, origen racial o vida sexual del interesado.

El Proyecto de LORTAD excluye de su ámbito a los ficheros de titularidad pública cuyo objeto sea el almacenamiento de datos para su publicidad **con carácter general,** inciso éste que permite someter íntegra y exclusivamente a la Ley de Procedimiento Administrativo, y en su caso a la legislación sectorial, los ficheros, aunque informatizados, a los que puedan acceder «los ciudadanos» (art. 105 C.E.) y no sólo los titulares de los datos.

Pero entre una y otra situación (datos que afecten a la intimidad, sujetos a la LORTAD; datos de documentos no nominativos y datos públicos, sujetos en su consulta a la Ley de Procedimiento y al derecho de acceso a los registros y archivos públicos y legislación sectorial) se encuentran aquellos otros **documentos nominativos** de carácter administrativo que, **sin incluir datos que afecten a la intimidad,** sólo pueden ser objeto de acceso y consulta por personas que acrediten un «interés legítimo» y cuyo régimen debe quedar sujeto a la Ley de Procedimiento Administrativo.

Intimidad y libertades

JOSE MANUEL MARTÍN BERNAL
Doctor en Derecho y en Ciencias Políticas y Sociológicas.
Magistrado. Profesor Titular de Derecho Civil

M.ª DEL PILAR MARTÍN GARCÍA
Licenciada en Derecho
(ESPAÑA)

SUMARIO

I. JUSTIFICACION DE LA RUBRICA
II. LA INTIMIDAD: SU AUTONOMIA Y SU RELATIVISMO
III. LA PROTECCION DE LA INTIMIDAD Y LA INFORMATICA
IV. EL CONVENIO DEL CONSEJO DE EUROPA
V. PROPUESTAS DE DIRECTIVAS COMUNITARIAS
A modo de conclusión.

I. JUSTIFICACION DE LA RUBRICA

Una rúbrica como la que encabeza el presente trabajo exige de entrada algunas consideraciones y precisiones previas en aras de un mejor entendi-

miento del tema que nos proponemos desarrollar y del método por el que nos conducimos en su exposición.

Sin entrar aquí en el estudio de la distinta nomenclatura de los derechos fundamentales o derechos de la personalidad, la consabida dificultad de su catalogación tanto en el Derecho interno como en el Derecho Comunitario, –debida su ausencia seguramente al clima político que rodeara su configuración–, y la asistematicidad de los mismos, también de las libertades, en el texto constitucional, cuyo emplazamiento e identificación dificultan un tratamiento científico y una aplicación jurisdiccional rigurosa, parece que el único criterio del legislador al agrupar los derechos y deberes de los ciudadanos en los tres capítulos que los enuncian, está fundado en la protección y garantías con que se los defiende.

El Capítulo segundo está dividido en dos secciones: la primera sección está cubierta con una enunciación que desde el punto de vista de la interpretación del texto –«los derechos fundamentales y las libertades públicas»– parece referirse a derechos y libertades humanas que se atribuyen a «todos», y tienen, como veremos, una protección reforzada a la que son aplicables todos los procedimientos de garantía previstos en el derecho contemporáneo.

Es en esa inevitable dialéctica y problemática entre derechos y libertades en la que se inscribe este trabajo.

Derecho a la intimidad personal (art. 18.1 de la Constitución), que se articula en la Ley Orgánica 1/1982 de 5 de mayo que desarrolla el precepto constitucional indicado y lo regula (también el honor y la propia imagen) con referencias constantes a la persona en el artículo 2º; vida íntima de las personas en el artículo 7.º, 1 y 2; vida privada de una persona o familia, datos privados de las mismas, o imagen de una persona, núms. 3, 4 y 5 del mismo precepto, y reducto familiar del domicilio de la persona, que es inviolable, como el artículo 18.2 de la Constitución se encarga de encarecer; artículos todos los anteriores que al traer causa de la dignidad (art. 10.1 de la Constitución), que se configura como pórtico de los mismos, suponen una anteposición básica –la persona misma–, a la vez que un prius lógico e histórico, también antropológico, respecto de las libertades que el Ordenamiento Jurídico (posterius) establece o debe establecer, como ha de verse; límites y cautelas en las libertades de información (contenidas en el artículo 20.1.2 de la Constitución), y sobre todo por la aparición, perfeccionamiento y progresiva utilización de las comúnmente llamadas «tecnologías de la información», o «tecnologías informáticas», aparecidas en los últimos decenios, sobre todo a partir de 1.981, y con concreta referencia constitucional en el núm. 4 del citado artículo 18, que reza «La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», y que se encuentra todavía sin desarrollo legislativo.

En la medida en que concuerden y se armonicen el aspecto impersonal «se garantiza», y el personalista del artículo 18.1 del texto, –no en balde primeros en el tiempo y en su redacción literal constitucional–, y el reconocimiento y consiguiente protección de otros derechos y libertades con menor énfasis garantista (Se protegen....), se conseguirá una utilización correcta de la informática; más allá, superando ésta a aquélla, utilizando la misma para fines ilegítimos o prescindiendo de la medidas de seguridad adecuadas, estaríamos, seguramente, en presencia del abuso o ejercicio antisocial-constitucional del Derecho (art. 7.2 del título preliminar del Código Civil).

II. LA INTIMIDAD: SU AUTONOMIA Y SU RELATIVISMO

Los Derechos de la intimidad personal se identifican en general, como es sabido, para proteger y garantizar este contenido: una esfera inderogable de libertad personal en que se desenvuelve la racionalidad y la libertad de la vida privada de los individuos.

Su contenido, como ya hemos indicado, está vinculado a la misma dignidad de la persona, en cuanto supone las condiciones mínimas para que los hombres desarrollen su inteligencia y libertad.

La vida privada íntima –se ha dicho– es como la atmósfera misma de la personalidad. Sin duda alguna todos los derechos que la protegen tienen un carácter individualista, porque lo que en ella se respeta es precisamente la autonomía privada de la vida individual.

Autonomía que no supone ni se identifica con absolutismo ni con automatismo judicial por cuanto la protección a los bienes de la personalidad (De Castro prefería «Derechos») ha de dispensarse dentro de una intensa relativización correlativa a la índole de los mismos; protección que se manifestará, de una parte, permitiendo extenderla a supuestos distintos de los casos enumerados en el artículo 7.º de la citada Ley 1/1982. Estos casos la atraerán, desde luego, pero a la manera de acaecimientos más significativos o frecuentes y ejemplificadores de agresiones ilegítimas a la intimidad, destacados del principio general del «alterum non laedere». No constituyen, sin embargo un «numerus clausus».

De otra parte, la denotada relativización con la que ha de otorgarse la protección se manifestará tratando la personalidad y correlativa intimidad de cada persona y, en cada caso, según las circunstancias, que operarán decisivamente antes del contraste o confrontación de la norma con la ocurrencia concreta: ésta, pues, será configurada, caracterizada e individualizada por o a través de esas circunstancias, escogiendo el Juez las más relevantes, eliminando su automatismo, quedando ampliada la esfera valorativa del Juez, a quién competerá antes y con preferencia a la subsunción del hecho con la norma, la construcción selectiva de aquella parcela o manifestación concreta

de la vida que conviene a aquella, ateniéndose a las pautas a que la ley remite en su artículo 2.º.1.

Y es que no puede olvidarse que la esfera de la intimidad personal está determinada de manera decisiva por las ideas que pertenezcan e imperen en cada momento en la sociedad, y por el propio concepto que cada persona, según sus actos propios, mantenga al respecto, y determine su comportamiento; expresiones de la Ley misma por las cuales queda encomendada al Juzgador la prudente determinación del ámbito de la protección en función de datos variables según los tiempos, sus usos sociales, y en razón de las pautas de comportamiento libremente escogidas y asumidas por cada persona.

Se emparenta con este planteamiento la puesta en relación entre los derechos de expresión y de comunicación informativa, pues los derechos consagrados en el artículo 20.1, apartados a) y d) presentan un diferente contenido y hasta diferentes límites y efectos, pues al paso que la libertad de expresión tiene por objeto pensamientos e ideas que abarcan incluso las creencias y opiniones, el derecho a comunicar y recibir libremente información versa sobre hechos que pueden denominarse como noticiables en el común sentir social, de tal modo que como ya precisara la Sentencia de 8 de julio de 1976 del Tribunal de Derechos Humanos y puntualizó la del Tribunal Constitucional de 23 de noviembre de 1983, la comunicación informativa a que se refiere el apartado d).1 del artículo 20 de la Constitución, versa exclusivamente sobre hechos pero con tal entidad específica que tales hechos puedan encerrar trascendencia pública a efectos de que sea real y evidente la participación de los ciudadanos en la vida colectiva, de tal forma que de la libertad de información –con su efecto reflejo y correlativo que supone el derecho a recibirla– es sujeto primario la colectividad y cada uno de sus miembros.

Y aunque no todo alegato en defensa de lo que se diga intimidad o vida privada será, como la legislación y nuestra jurisprudencia muestran, merecedor de tal aprecio y protección, sí es preciso, señala la Sentencia del Tribunal Constitucional de 14 de febrero de 1992, reiterar ahora que la preservación de este reducto de inmunidad sólo puede ceder cuando del derecho a la información se trata, si lo difundido afecta, por su objeto y por su valor, al ámbito de lo público, no coincidente, claro es, con aquello que pueda suscitar o despertar meramente la curiosidad ajena. Y es que la libertad de información, al menos la que incide en el honor de las personas privadas, debe enjuiciarse sobre la base de distinguir radicalmente, –a pesar de la dificultad que comporta en algunos supuestos–, entre información de hechos y valoración de conductas personales, y, sobre esta base, excluir del ámbito justificador de dicha libertad las afirmaciones vejatorias para el honor ajeno, en todo caso innecesarias para el fin de la información pública en atención al cual se garantiza constitucionalmente su ejercicio.

III. LA PROTECCION DE LA «INTIMIDAD» Y LA INFORMATICA

Las reflexiones expuestas hasta aquí referidas a la libertad de información e intimidad resultarían incompletas, sin las que han de concordarse y armonizarse entre el derecho a la intimidad y su protección y el tratamiento automatizado de la misma.

No resulta fácil ni ser breve ni sistemático, y en todo caso original en un tema como el de la informática, sometido a múltiples estudios, proyectos y textos legales ya promulgados en distintos países, abordado con diversos enfoques y perspectivas respecto de los campos que acota; su incidencia es distinta según la disciplina jurídica que lo irradie, y hasta el de sectores o tipo de personas que pueden comprender, y, sin embargo, resulta obligado e imprescindible establecer ahora algunas consideraciones en cuanto a las libertades que pueden atacarse y a la preservación del derecho que venimos estudiando.

Un estudio comparativo de las legislaciones nacionales e internacionales muestra que se han tomado una serie de medidas para conciliar esa suerte de contradicción que acaba de indicarse, contradicción que también se advierte de entrada cuando se cuestiona a la informática en sí o a la utilización que de la misma pueda hacerse para fines ilegítimos o prescindiendo de las medidas de seguridad adecuadas, y es que en el tema se confunde a menudo la mala noticia con el mensajero. Como señala Joaquín de la Llave «sería cuestionable que la protección de la informática debiera ser diversa de la genérica frente al empleo abusivo de informaciones por medios no informáticos ni automatizados». En este sentido, es importante que las posturas «visceralmente contrarias a la expansión informática claudiquen ante un hecho que hoy es irreversible y ajusten sus esfuerzos a encauzar su uso dentro de los límites marcados por el respeto a los derechos fundamentales de la persona».

En cualquier caso, la preocupación existe, y a ella se ha intentado dar respuesta jurídica desde instancias tanto nacionales como internacionales, si bien de forma diversa en el tiempo, en el contenido, en las distintas legislaciones, disponiendo la creación de órganos encargados de velar por la correcta utilización de ficheros públicos y privados de datos personales, así como de la Jurisprudencia escasa y ausente al respecto por la problemática antes apuntada.

El contenido de las leyes aprobadas presenta diferencias en función de variables tales como las peculiaridades de los sistemas judiciales y la tradición jurídica de cada país.

No es este el momento para descender al estudio de leyes generalistas,-básicamente en el Derecho europeo, que indagan en la casuística por contra de lo que sucede en EEUU, impregnadas de un mayor pragmatismo, aprobando regulaciones específicas para los diferentes sectores, tanto a nivel fede-

ral como estatal, lo que convierte al sistema de protección estadounidense en un modelo profundamente distinto del europeo.

Tampoco es nuestro propósito entrar ahora en detalles de los distintos sistemas judiciales europeos, que también otro Magistrado ha puesto recientemente de manifiesto (José María Alvarez Cienfuegos Suarez, en Aranzadi N.º 4 julio 1992). Pero ello no nos impide tomar conciencia de que ante el nacimiento de un mercado telemático europeo acorde con el mercado único, el Derecho, y particularmente los juristas, tendrán que conciliar, en lo que a la circulación de datos se refiere, aspectos tan diversos como el respeto a la vida privada, el acceso a los sistemas de información, los intereses generales de los Estados, su alcance, su protección, control o garantía, sus límites y sus excepciones, con las distintas acepciones y la semántica que pone de manifiesto cómo el pluralismo terminológico se muestra tanto como exponente de la riqueza lingüística, como obediente a la dificultad que encierra el tema.

Y otro tanto pudiera decirse de la Jurisprudencia del Tribunal de Justicia de las Comunidades, que erigido en auténtico garante de la protección de los derechos fundamentales (otra cuestión es cuáles, cuántos y de qué naturaleza) ha buscado por sí mismo la solución del problema de la protección de los mismos, creando Derecho por medio de la acuñación de los Principios Generales del Derecho Comunitario (ver por todas y referidas al derecho de la intimidad la sentencia Stauder de 12 de noviembre de 1969: asunto 29/69, y la sentencia National Panasonic, de 26 de junio de 1980, asunto 136/79).

IV. EL CONVENIO DEL CONSEJO DE EUROPA

El contenido del Convenio se inspira en gran parte en leyes nacionales aprobadas en años anteriores, y, a su vez, ha inspirado el contenido de leyes nacionales posteriores. Como en muchas de éstas, se ha preferido enunciar principios generales de protección, sin descender al detalle sectorial.

En el artículo 1.º se expone claramente el objetivo que se persigue:

«El fin del presente Convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.»

Para conseguir este objetivo se fijan una serie de principios básicos. Así, el Convenio exige que los datos de carácter personal objeto de un tratamiento automatizado:

– se obtengan y traten leal y legítimamente;

– se registren para finalidades determinadas y legítimas y no se utilicen de forma incompatible con dichas finalidades;

– sean adecuados, pertinentes y no excesivos en relación con estas finalidades;

– sean exactos y puestos al día;

– se conserven durante un período de tiempo que no exceda del necesario.

Además de estas cautelas generales, cuando se trate de datos que revelen el origen racial, opiniones políticas o religiosas o datos relativos a la salud o la vida sexual, se prohíbe su tratamiento salvo que el Derecho interno del país firmante prevea garantías apropiadas.

Entre los aspectos tratados de mayor importancia destacan las garantías complementarias de la persona concernida. Cualquier persona deberá poder:

– conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades, así como la identidad y residencia o establecimiento de la autoridad controladora del fichero;

– obtener, a intervalos razonables y sin demora o gastos excesivos, la confirmación de la existencia de sus datos personales en el fichero y la comunicación de dichos datos en forma inteligible;

– obtener, en su caso, la rectificación de los datos;

– disponer del recurso pertinente si no se atienden sus peticiones.

La amplitud de estos derechos obliga a introducir algunas excepciones para casos concretos. Así, el Convenio posibilita la excepción cuando sea necesaria para la protección de la seguridad del Estado o de la seguridad pública, para los intereses monetarios del Estado, para la represión de las infracciones penales y para la protección de la persona concernida o los derechos y libertades de otras personas.

Por otra parte, y aunque el objetivo perseguido sea la protección de derechos fundamentales de la persona frente a un tratamiento automatizado de los datos que le conciernen, el Convenio abre la puerta a una extensión de su aplicación por parte de los Estados a las informaciones relativas a agrupaciones, asociaciones, fundaciones, compañías u otro organismo compuesto directa o indirectamente de personas físicas. También prevé la posibilidad de aplicar sus normas a ficheros de datos que no sean objeto de tratamiento automatizado, sino manual.

En definitiva, la aprobación del Consejo de Europa supuso un gran avance en el cambio hacia la unificación de criterios en esta materia, estableciendo, además, niveles de protección que pueden calificarse de notables.

V. PROPUESTAS DE DIRECTIVAS COMUNITARIAS.

Ya en el año 1981 la Comisión recomendaba a los Estados Comunitarios la ratificación del Convenio Consejo de Europa. Dado que esa ratificación

no ha sido efectuada por todos los Estados miembros, se han puesto en marcha varias iniciativas legislativas en materia de protección de datos personales. Entre estas iniciativas, la de mayor importancia es la propuesta de Directiva del Consejo sobre la protección de las personas respecto al tratamiento de datos de carácter personal. Otras iniciativas sobre seguridad de la información pueden considerarse como complementarias de aquélla.

El objetivo fundamental, es evitar que la existencia de distintos niveles de protección en cada país pueda perjudicar la libre circulación de datos de carácter personal.

Considerado en su conjunto, el Proyecto aborda la regulación de la protección de datos con pretensión generalizadora, si bien prevé la posibilidad de que la Comisión apruebe las normas técnicas necesarias para aplicar la Directiva a sectores específicos. Se sigue en este punto la «tradición europea» de preferir una norma general frente a la dispersión de la normativa sectorial.

Quizá el capítulo IV sea el de más concreta aplicación al tema que nos ocupa por cuanto se dedica a la regulación de los derechos de la persona concernida. En él se reitera la necesidad del consentimiento del afectado y se establecen las cautelas pertinentes para lograr que este consentimiento no esté viciado y sea válido. Asimismo, se determina la obligación de informar al afectado en un momento especialmente delicado: el de la obtención de los datos. Por último, se enumeran una serie de derechos complementarios de extraordinaria importancia. Así, entre otros, el derecho a oponerse por razón legítima a que los datos sean objeto de tratamiento, a conocer la existencia del fichero y sus finalidades principales, a obtener la rectificación de datos inexactos y, muy especialmente, a obtener en intervalos razonables la comunicación de una forma inteligible de los datos personales que figuran en un fichero.

Al igual que ocurría en el Convenio del Consejo de Europa la magnitud de tales derechos exige el establecimiento de excepciones puntuales. En este sentido, la Propuesta prevé la posibilidad de limitarlos mediante ley por motivos relativos a la seguridad y defensa del Estado, la seguridad pública, la persecución penal, el interés económico o financiero de un Estado miembro de la Comunidad, la necesidad del ejercicio de funciones de control o inspección de la autoridad pública, o un derecho equivalente de otra persona o los derechos y libertades de otro.

En resumen, puede afirmarse que, en la hipótesis de aprobación de un texto similar al del Proyecto, la Directiva supondrá un nivel de protección superior al derivado del Convenio del Consejo de Europa.

En el caso español, el Proyecto de Ley de protección de datos responde a los criterios seguidos por la legislación aprobada de otros países comunitarios, y ha de suponerse que tampoco ha de plantear graves problemas su adaptación al texto comunitario, aunque ya algunas de las cuestiones tratadas

han despertado recelos en determinados ámbitos. En particular, los Estados Unidos han mostrado su preocupación por las limitaciones en la transferencia de datos a terceros países en caso de que no se garantice un nivel de protección equivalente al comunitario.

A MODO DE CONCLUSION

Debemos terminar, pero no sin hacernos eco de algunos sueltos publicados bien recientemente en la prensa española. Por conocidos, nos limitamos a enunciar algunos de sus títulos, cuyos contenidos revelan posibles atentados contra la intimidad: «Buen negocio para telefónica», «Telefónica vende datos personales de sus abonados a empresas de publicidad directa»..., que pueden entrañar un abuso y un fraude, en cuanto que se trata de datos obtenidos para fines exclusivos de telefónica que pueden configurarse no ya sólo como abuso de su posición dominante ante la indefensión del usuario ante tales hechos, cuya práctica ha sido puesta en conocimiento del Defensor del Pueblo, también a través de denuncia ante el Fiscal General del Estado por la OCU, en queja formal por lo que considera revelación privada de datos e intromisión ilegítima de las personas. Un portavoz de Cetesa afirma que los datos que comercializa son públicos y que no vulneran la legalidad vigente. Y es que en esa encrucijada entre lo privado y lo público, si es que hoy puede hablarse en esos términos, se halla nada más pero nada menos, que la intimidad de las personas que se garantiza en el artículo 18.1 de nuestra Constitución.

Las obligaciones y las responsabilidades del titular de un fichero de datos nominativos en cuanto a la cualidad de su producto

ETIÉNNE MONTERO
Maître de Conférences
Profesor de Derecho de la Facultad de Droit de Namur
(BELGICA)

Palabras claves:

Bancos de datos-Productor-Responsabilidad del productor-Jurisprudencia «clásica» relativa al suministro de informaciones-Evolución en el contexto de los bancos de datos-Informaciones nominativas-Legislaciones «privacy» y derecho común de la responsabilidad.

1. *Introducción.*–Esta comunicación plantea la cuestión de la incidencia de las legislaciones «privacy» sobre el régimen de responsabilidad de los productores (P) de bancos de datos (BD) que contienen informaciones nominativas.

Con este fin, después de haber resaltado las obligaciones puestas a cargo de los proveedores de información por la jurisprudencia «tradicional», nos interrogamos sobre el porvenir de los criterios de responsabilidad en el nuevo contexto de los servicios electrónicos de información.

A continuación, nos preguntaremos si las legislaciones «privacy» dejarán a salvo este derecho común de la responsabilidad o si, al contrario, lo modificarán.

2. *El productor es responsable del contenido del BD.*–En el derecho de los bancos de datos, se llama «productor» al que está en el origen de la

creación del banco de datos, y que concibe el modo de desarrollarlo. Es el que «gestiona, amontona y estructura las informaciones que recoge o genera para proponer al usuario un producto documental acabado y con valor añadido» [1].

Dueño del sistema de informaciones, responsable de su generación o recolección y de su organización, el productor del BD ha de ser responsable de su contenido. Este principio está admitido por todos los autores [2].

3. *La jurisprudencia clásica.*–Para exponer el régimen de responsabilidad del productor en caso de suministro de informaciones defectuosas, parece lógico referirse a la jurisprudencia ya existente.

En efecto, el suministro de informaciones no constituye un fenómeno nuevo derivado del desarrollo de los servicios electrónicos de información.

Desde hace ya mucho tiempo informaciones comerciales son suministradas por las agencias de información comercial y por los bancos mientras que informaciones administrativas son suministradas por las administraciones públicas. La jurisprudencia existente en Francia y Bélgica en estos campos es abundante.

A continuación, trataré de apuntar las obligaciones que la jurisprudencia pone a cargo de los proveedores de información y de perfilar su régimen de responsabilidad.

Aunque hay matices en la jurisprudencia según el sector (agencias, bancos, administraciones, ...), no nos parece útil mencionarlas en el marco limitado de esta comunicación.

A propósito de los fundamentos posibles de la responsabilidad, nos limitaremos a señalar que está en principio contractual [3] frente al destinatario de la información y delictual frente a los terceros entre los cuales contamos a las personas a las que se refiere la información.

Después de haber expuesto el contenido y la naturaleza de las obligaciones a cargo de los proveedores de información, precisaremos los distintos momentos en los que se aprecia el cumplimiento o incumplimiento de dichas obligaciones.

El proveedor de información tiene la obligación de suministrar informaciones exactas, actuales y exhaustivas.

---

[1] N. POUJOL, «La commercialisation des banques de données», thse, 1992, p. 355; v. también Groupement français des fournisseurs d'information en ligne (GFFIL), Les relations contractuelles des producteurs de bases et banques de données, Dalloz, 1986, p. 22.

[2] P.ej. S. DENIS, Y. POULLET et X. THUNIS, Banques de données: quelle protection juridique?, Cahiers du Centre de Recherches Informatique et Droit, nº 2, Story scientia, 1988, p. 15; también S. SCHAFF, Banques de données juridiques: analyse des contrats proposés aux utilisateurs, D.I.T., n.º 7, 1985, p. 3.

[3] Existe sobre este punto una controversia.

4. *Obligación de exactitud.*–La obligación de exactitud, en la jurisprudencia clásica, debe ser entendida en términos de «contenido intelectual» de la información.

Cuando aún no estaba automatizado el suministro de informaciones, prácticamente era excepcional que la inexactitud proviniese de una falta imputable a una operación de tipo técnico.

Al contrario, la inexactitud de una información conseguida por la consulta de un BD proviene más frecuentemente de un error material relacionado con una operación del tratamiento automatizado de la información: recolección, grabación, almacenamiento, modificación, supresión o transmisión. Dicho de otra manera, con el desarrollo de los servicios electrónicos de información asistimos a una multiplicación de hechos generadores de inexactitud. Y mientras la inexactitud intelectual de la información es a menudo imputable a la falta del proveedor, es más difícil determinar si la inexactitud puramente material es imputable al hombre o a la «máquina».

Tradicionalmente, la exigencia de exactitud prohibe la difusión de informaciones falsas, incompletas, parciales o ambiguas [4].

Se encuentran muchísimos ejemplos en la jurisprudencia en los que el proveedor de informaciones ha sido declarado responsable por haber difundido una información falsa (es decir contraria a la verdad objetiva), parcial o ambigua.

Demos unos ejemplos:

– la información de que un procesado había cometido una estafa mientras se beneficiaba de la presunción de inocencia [5];

– el anuncio del fallecimiento de alguien que no había muerto [6];

– información inexacta sobre la situación hipotecaria de alguien [7];

– la información de que una empresa era copropietaria de un inmueble, lo que era falso [8].

Una información puede ser inexacta por ser incompleta. Así el uno de marzo de 1982, el Tribunal Supremo de Francia ha aprobado una Sentencia de un tribunal de apelación condenando una agencia de información comercial que, respecto a la situación económica de una empresa, había indicado sólo elementos favorables omitiendo los desfavorables [9]. Profundizaremos más adelante, hablando de la exhaustividad, esta obligación de comunicar informaciones completas.

---

(4) N. POUJOL, op. cit., n.º 440-443.
(5) Cass. civ., 16 juin 1986, citado por N. POUJOL, op. cit. n.º 438.
(6) Trib. civ. Seine, 19 juin 1963, J.C.P., 1963, ed. G, II, 13.379.
(7) Lige, 9 oct. 1985, Pas., 1986, III, 6; Civ. Charleroi, 2 mars 1884, Pan. Pér., 1438.
(8) Cass. fr., 14 mars 1978, D. 1979, 549, obs. TENDLER.
(9) Cass, fr. 1er mars 1982, Gaz. Pal, 1982, 2, Pan. 250, obs. CHABAS

5. *Obligación de «actualidad».*–Varias sentencias atestiguan la obligación para el proveedor de informaciones de difundir informaciones actuales. Es difícil apreciar esta obligación en la medida en que el concepto de actualidad de la información parece ser relativo y subjetivo. La «diligencia debida» por el proveedor dependerá de las posibilidades reales de acceso a la información más reciente. El carácter actual de la información dependerá también de las intenciones del destinatario: para qué solicita la información y qué quiere hacer con ella. Una información puede ser para la mayoría suficientemente actual y sin embargo ya obsoleta para tal destinatario. A ese respecto, el concepto de «espera legítima» por parte del destinatario puede ser de un gran interés.

Para ilustrar esa obligación de actualidad, nos limitaremos a mencionar la sentencia del 30 de enero de 1974 del Tribunal Supremo de Francia. Confirma la sentencia de los jueces de apelación que han decidido que una agencia de información comercial había cometido una falta al suministrar una información sin emitir ninguna reserva a pesar de que tenía «informaciones obsoletas, que remontaban a más de 6 meses» [(10)].

Consideremos que en el contexto de los servicios electrónicos de información, on line sobre todo, la exigencia de la actualidad de la información es habitualmente muy importante para el usuario.

Además, los términos del problema son distintos. La cuestión de la actualidad de la información llega a ser la de la actualización o puesta al día del BD. El contenido de esta «nueva» obligación dependerá de factores técnicos a veces no imputables al productor.

Si se puede reprochar a una agencia de información comercial no haber controlado una información, pidiendo por ejemplo confirmación por teléfono, este reproche es menos concebible cuando se trata de un productor de BD. El volumen de las informaciones recogidas, tratadas, almacenadas y puestas a disposición de los clientes así como el carácter despersonalizado de la interrogación on line dificultan este tipo de aproximación.

Finalmente, observemos que, en principio, es poco razonable pretender para todos los BD una puesta al día en tiempo real por el motivo que la interrogación se hace en tiempo real. El concepto de «plazo razonable» será al contrario muy útil. Una obligación de resultado en cuanto a la actualidad de la información sólo se concibe en la hipótesis en que el productor se haya comprometido sobre un plazo preciso de puesta al día.

6. *Obligación de exhaustividad.*–Algunas sentencias han sancionado el defecto de exhaustividad de la información en el campo de la edición. Así, el Tribunal civil de Nantes ha declarado fundada la acción en responsabilidad dirigida contra una asociación de resistentes, con el motivo que «hablando

[(10)] Cass. com., 30 janv. 1974, D., 1974, 428, obs. TENDLER.

de la actuación de la resistencia sólo había mencionado los excesos culpables de algunos omitiendo de informar honestamente sus lectores sobre la actuación patriótica de los demás» [11].

El caso «Branly» (una sentencia del Tribunal Supremo del 27 de febrero de 1951) es el más famoso de la falta por omisión en la información. Fue reprochado a un historiador no haber mencionado el nombre de Branly entre los sabios que habían contribuido a los progresos de la telegrafía inalámbrica [12].

En estos distintos casos [13], la evaluación de la cualidad de la información resulta muy peculiar en cuanto están implicadas las libertades públicas, de opinión, de expresión, de edición... Desde este punto de vista, en estos casos, sólo puede presentarse el derecho de la responsabilidad civil como el arbitraje de un conflicto de valores: libertad de opinión, por una parte, derecho a la información, por otra parte. El tratamiento de este conflicto debe pertenecer al juez.

Dejando de lado esta cuestión, sólo indicaremos que, en el contexto de los BD, el problema de la exhaustividad está modificado. Tal obligación está desplazada: no es ya una cualidad de la información «en sí» sino del BD en su conjunto.

A este respecto, la presentación del BD es de suma importancia. No todos los BD pretenden ser exhaustivos. Un productor de BD puede decidir ofrecer un banco de datos no exhaustivo e indicarlo en la descripción del «corpus».

Por eso perdió la asociación francesa BGP su proceso. Quería que un proveedor fuese condenado porque su banco de datos sólo ofrecía informaciones sobre empresas industriales cuando buscaba informaciones sobre empresas comerciales. El Tribunal de París juzgó que este punto había sido mencionado previamente en la descripción del BD.

La utilización de las técnicas documentarias típicas de los BD suscitan también preguntas. Por ejemplo, ¿como apreciar el carácter completo o exhaustivo de un abstract o de un resumen? La utilización masiva de estas técnicas para condensar la información multiplica el riesgo de comunicación de informaciones inexactas, ambiguas (resumiendo se pierden matices...), parciales (porque hay que elegir), incompletas...

7. *Naturaleza de las obligaciones.*–En cuanto a la naturaleza de las obligaciones que incumben al proveedor de información, los autores y la jurisprudencia juzgan que «el suministro de información tan sólo debe poner a cargo de aquél una obligación de «medios», de prudencia y diligencia. El solo hecho de suministrar una información inexacta no basta para que el

[11] Triv. civ. Nantes, 23 oct. 1953, J.C.P., 1954, 7993, obs. TENDLER.
[12] Cass., 27 févr. 1951, D., 1951, 329, obs. DESBOIS.
[13] V. también Triv. civ. Chaumont, 13 mai 1946, D., 1947, 53, obs. LALOU.

proveedor pueda ser declarado responsable; además hay que establecer una falta, al menos de «negligencia». Formalmente, los tribunales adoptan el criterio de la obligación de «medios». Pero un análisis más fino de la jurisprudencia revela que dicha obligación está apreciada con un rigor extremo, quasi como si fuera una obligación de resultado.

Esta observación es especialmente válida en el campo de las agencias de información comercial (profesionales de la información que actúan a cambio de una remuneración) [14], sobre todo, cuando se trata de suministrar informaciones precisas y objetivas.

8. *Evaluación de la falta.*–Las obligaciones apuntadas pueden ser apreciadas en los dos niveles de la actividad de información: la recolección y la difusión. La falta del proveedor de información puede situarse en el momento y en la manera de reunir (o producir) la información o en el momento y en la manera de comunicarla.

En cuanto a la recolección se destaca la obligación de «investigar lo suficiente», la obligación de «dirigirse a gente competente y a fuentes dignas de confianza». Y la obligación de control («hacer verificaciones normales») que es especialmente «importante» cuando se trata de una «información desfavorable».

El proveedor de información debe también rectificar con diligencia las informaciones erróneas cuando se le advierte.

En cuanto a la comunicación, el proveedor de información también tiene que respetar una serie de obligaciones. Así en caso de duda, tiene la obligación de «formular reservas». Puede tener la obligación de «indicar la incertidumbre sobre la información suministrada» o de «no presentar una información dudosa como precisa o categórica».

Si una información ha sido dada por un tercero, sin posibilidad de controlarla, existe obligación de indicar claramente que «proviene de un tercero».

También hay que mencionar la obligación de «llamar la atención del cliente sobre las controversias» relativas a la información comunicada.

9. *¿Hacia una responsabilidad objetiva?*–No es necesario subrayar que muchos de estos criterios de apreciación de la falta del proveedor de información no sirven ya en el contexto de los BD. La despersonalización del servicio, la multiplicación de hechos generadores de daños, los riesgos de fallos puramente técnicos, las dificultades de imputabilidad... son factores que dejan ver una evolución probable de la jurisprudencia hacia una responsabilidad objetiva.

10. *Legislaciones «privacy» y derecho común de la responsabilidad.*– Ahora bien ¿qué hemos de pensar de esta tendencia si integramos en el debate

[14] Mientras que los bancos y las administraciones públicas suministran habitualmente las informaciones perdidas, gratuítamente y en el marco de un servicio accesorio.

una reflexión sobre la protección de la vida privada frente al tratamiento de datos nominativos?.

Se trata de saber si las legislaciones «privacy» tienen una incidencia sobre el derecho común de la responsabilidad civil del P. de BD respecto a la cualidad de la información. Las obligaciones creadas por estas legislaciones ¿están destinadas a modificar el contenido y la naturaleza de las obligaciones que incumben tradicionalmente a los proveedores de información?

El concepto de «información nominativa» debe entenderse en el sentido de la Convención nº 108 del Consejo de Europa [15] como «toda información relativa a una persona física identificada o identificable».

La interpretación extensiva dada a esta noción [16] implica que serán numerosos los BD sometidos a estas legislaciones «privacy».

De ordinario, estas legislaciones ponen a cargo del titular del fichero 4 obligaciones importantes: la obligacion de declarar la finalidad del tratamiento, la obligación de informar a las personas fichadas de la existencia del fichero y de su finalidad, la obligación de organizar un derecho de acceso, la obligación de rectificar los datos inexactos que esten señalados.

Estas tres últimas obligaciones pueden analizarse como obligaciones de resultado en el sentido en que el P. del BD es automáticamente responsable –también a menudo penalmente– si una de estas obligaciones queda sin cumplir.

El principio de finalidad implica que los datos tratados por el P. sean adecuados, pertinentes y no excesivos de acuerdo al fin invocado. También significa que su conservación no debe exceder las necesidades de atender a ese fin. A este respecto, notemos que la obligación de suministrar informaciones completas lleva consigo un matíz muy específico. En efecto, el carácter completo o incompleto de la información se define en referencia a un criterio preciso que es la finalidad del tratamiento. Así, en el artículo 14 del proyecto belga de ley sobre la protección de la vida privada frente al tratamiento de datos nominativos, se trata del derecho a exigir la rectificación o supresión «de todo dato nominativo inexacto o, teniendo en cuenta la finalidad del tratamiento, incompleto y no pertinente».

Respecto a la exactitud, las legislaciones «privacy» prevén explícitamente que «los datos deben ser exactos y, en su caso, actualizados» [17].

La cualidad de los datos tratados está garantizada por el dispositivo de protección –información, acceso, rectificación organizado por las legislacio-

---

[15] Convención del Consejo de Europa del 28 de enero de 1981, n.º 108.

[16] V. por ej. L. COSTES, Informatique, fichier et vie privée, Actas del Congreso internacional Informática y Derecho, Buenos Aires, 16-19 de octubre de 1990, espec. n.º 9 p. 528-529; V. VIVANT, Chr. LE STANC, L. RAPP et M. GUIBAL, Lamy Droit de l'Informatique, 1992, n.º 1149 y s.

[17] Art. 5, D de la Convención del Consejo de Europa, 28 de enero de 1981.

nes «privacy» con el fin de evitar los riesgos de daño a la intimidad de las personas fichadas.

Notemos que en principio el sistema garantiza también indirectamente la cualidad de la información con respecto al destinatario. Investido del derecho de acceso y de rectificación de los datos que la conciernen, la persona fichada está llamada a participar indirectamente pero activamente en el proceso de elaboración de un «producto informacional» de cualidad. Dicho de otra manera, la persona fichada aparece como un «guardian de la exactitud» junto con el productor. En consecuencia, parece razonable sostener que la responsabilidad en relación con la cualidad de la información esta en parte desplazada del productor hacia la persona fichada.

Por lo tanto, se pasaría de un sistema de responsabilidad fundamental unilateral –en el que el P. es el único garante de la exactitud– a la institucionalización de un sistema de responsabilidad compartida.

¿Cuál sería la traducción concreta de esta manera de enfocar la cuestión? ¿Sería imaginable que una acción en responsabilidad civil fuese introducida por el destinatario de una información inexacta contra la persona fichada que hubiera omitido el ejercicio de sus derechos de acceso y rectificación? O más sencillamente, en la misma hipótesis, el productor responsable de haber suministrdo una información inexacta ¿debe tener un recurso automático contra el tercero fichado?

Admitir que tal omisión pueda ser una falta supone, en los dos casos, que los derechos otorgados a la persona fichada se interpreten como verdaderas obligaciones.

En la medida en que el control de la exactitud incumbe también a la persona fichada ¿deben ser el productor y esta última solidariamente responsables frente al destinatario?

11. *Consideraciones finales.*–Evidentemente en el estado actual de la práctica y del derecho, no parece que esta curiosa orientación sea confirmada. Resulta que frente a las legislaciones «privacy» el productor de un BD conteniendo informaciones nominativas no puede ser ya percibido como el único dueño de la cualidad de su producto. A este respecto, se piensa en la hipótesis en que, ejerciendo un derecho de acceso y de rectificación, el tercero comunica voluntariamente informaciones inexactas (más favorables por ejemplo) sobre sí mismo.

Estas observaciones no contradicen necesariamente la tendencia jurisprudencial a favor de una responsabilidad objetiva de los proveedores de información frente a sus destinatarios.

Lo único que hoy en día parece cierto es que la persona fichada asume una parte de la responsabilidad en cuanto a la cualidad del producto. ¿En qué proporción y con qué título exactamente? Son preguntas que la doctrina jurídica deberá enfocar en un porvenir próximo.

Bases de datos, privacidad y responsabilidad civil

JOSEFINA C. ORZABAL

Doctora en Ciencias Jurídicas y Sociales
Profesora adjunta de Derecho Civil II
Facultad de Derecho de la Univ. Nac. de Rosario
Presidenta del Instituto de Derecho Informático
Colegio de abogados de Rosario
(ARGENTINA)

I. INTRODUCCION

Fundamentalmente a partir de su convergencia con la telecomunicación, lo que dio lugar al surgimiento de las nuevas tecnologías telemáticas que integran las tecnologías de la información, la informática ha llegado a constituirse en infraestructura del quehacer moderno, haciendo de la nuestra la sociedad de la información. Bases de datos y redes telemáticas que captan, procesan inmediatamente y trasmiten velocísimamente cantidades ilimitadas de datos avanzan cada día con su avasallante poder sobre un nuevo sector de nuestra vida, se apoderan de datos que nos conciernen y llegan a amenazar nuestros derechos y libertades. Esta intrusión en nuestra vida privada que la informática permite –y que no es sino uno de los inevitables aspectos de la proyección social del desarrollo tecnológico confiere nuevos perfiles al derecho a la privacidad, a la vez que nos señala la necesidad de fortalecer los fueros de este principio a fin de lograr que, fundamentalmente, la tecnología informática sirva al progreso de la libertad del hombre.

El derecho a la privacidad, a la vida privada o a la intimidad, a la «privacy» es, como decía el eximio jurista argentino Alfredo ORGAZ «un problema muy siglo veinte», que no conocieron, al menos con parecida intensidad, los siglos anteriores. El hombre actual está expuesto, ya no solamente a violaciones de su integridad física, de su libertad externa y de su propiedad sobre bienes materiales, sino a intromisiones en un ámbito mucho más suyo y recatado: su intimidad» [1].

II. EVOLUCION DEL CONCEPTO DE «DERECHO A LA VIDA PRIVADA»

Desde su primera formulación como un derecho subjetivo –el del individuo a permanecer aislado, sustraído al control social– hasta nuestros días, el derecho a la privacidad ha experimentado una interesante evolución, que se advierte en el diverso contenido que su concepto ha presentado a través del tiempo.

1. El derecho a la intimidad como derecho subjetivo. «The right to be let alone».

Aunque poco conocido, al parecer el primer texto que hizo mención del derecho a la vida privada fue el Real Decreto español del 10 de abril de 1852, que establecía que: «Delinque contra los particulares ... 2º el que aún sin cometer injurias ni calumnias da a luz, sin el asentimiento del interesado, hechos relativos a la vida privada y extraños de todo punto a los negocios públicos». [2]

Sin embargo, por su incidencia en el pensamiento jurídico contemporáneo, debido al desarrollo que –sobre su base– hicieron del tema los tribunales norteamericanos, es un artículo de Samuel D. WARREN y Louis B. BRANDEIS titulado, precisamente, «El derecho a la privacidad» (publicado en 1980 por la Harvard Law Review) el que ha trascendido como primera formulación del derecho a la intimidad [3].

Este artículo, concebido como reacción a la intromisión periodística en la vida del señor Warren –mundano y dispendioso hombre de negocios– reclamaba para el individuo the right to be let alone, el derecho a ser dejado solo o, como podríamos decir en una expresión vulgar, el derecho a ser dejado en paz.

El derecho a la vida privada fue, pues, enunciado en un comienzo con un enfoque netamente individualista, al punto que en las primeras elaboraciones

---

[1] ORGAZ, A., «La ley sobre intimidad», *El Derecho* Tomo 60, pp. 930 y ss.

[2] ROTMAN, R., nota bibliográfica sobre el artículo de Roberto Golschmidt «La protección jurídica de la vida privada», citado por RAMELLA, P., «El derecho a la intimidad», *La Ley,* Tomo 140 pp. 1172.

[3] GOLDENBERG, I., «La tutela jurídica de la vida privada», *La Ley,* 1976, A, pp. 578 y ss.

conceptuales fue diseñado con un perfil casi idéntico al del derecho de propiedad, en cuanto derecho del individuo al uso exclusivo de un bien.

2. El derecho a la intimidad como libertad informática: «Del secreto al control».

En los países tecnológicamente avanzados, a partir de la década pasada, esa concepción del principio de privacidad que autorizaba al individuo a ser tratado como una isla en la sociedad hubo de ceder frente a los profundos cambios producidos por las tecnologías informáticas. La informatización del tejido social había ya dado lugar al nacimiento de potentes bases de datos (fundamentalmente las de la administración pública, operadas tanto por los organismos de seguridad como por los prestadores de servicios sociales) cuyo nutriente era, precisamente, información concerniente a los individuos.

La revolución tecnológica, al introducir el tratamiento de los datos a nivel masivo, imprimió necesariamente al principio de privacidad un contenido muy distinto: por una parte, por la fuerza de los hechos, el individuo tuvo que participar en la remodelación de la organización social introducida por la informática, lo que le significó tener que proporcionar sus datos para participar de los beneficios de las nuevas actividades y entidades surgidas con tales tecnologías, renunciando a la reserva en que hasta entonces había mantenido a muchos de ellos. Ejemplo de ello son las prestaciones sanitarias, educativas, obras sociales, etc., que son organizadas en base al procesamiento de los datos de sus beneficiarios, proporcionados por ellos mismos.

Por otro lado, en los bancos de datos los peligros de agresión a la privacidad se concentran y ya no se trata sólo de la lucha de un particular contra otro para evitar intromisiones indiscretas en los propios actos: el individuo se enfrenta hoy con potentes organizaciones que, al combinar los datos, pueden ser fuente de daños y de violaciones a su intimidad.

De tal modo, el derecho a la privacidad ha venido evolucionando desde aquella primera pretensión del individuo de ser dejado sólo, de excluir a los demás de información sobre sí mismo, a lo que hoy se conoce como «libertad informática», esto es, la libertad del particular de controlar la información nominativa que le concierne cuando ella está contenida en un centro electrónico de datos.

Condensando esta nueva concepción del derecho a la privacidad, destaca el jurista italiano Enzo ROPPO un expresivo «slogan» que constituye tanto una rediseño del principio como una indicación de política legislativa: «del secreto al control». «Del secreto al control, éste el slogan que podría acompañar las nuevas tentativas de construir la tutela de la privacy adecuada a la evolución a que han llegado las tecnologías informáticas en su presente desarrollo. La tutela de la privacy no puede ser una «tutela de tipo propietario» sino que se torna una tutela de tipo «procedimental». No se trata de simplemente prohibir a la generalidad de los sujetos la recolección y el uso

de informaciones que se refieren a una determinada persona y, por así decir, «le pertenecen» de una manera exclusiva; se trata, en cambio, (y es una operación jurídicamente más compleja) de canalizar la inevitable actividad de recolección y uso de la información sobre la base de modalidades, procedimientos, garantías, controles, que ofrezcan la razonable certeza de que de estas informaciones no se hará un uso impropio [4].

La legislación surgida en los países desarrollados a partir de 1970 para dar respuesta eficaz específicamente al problema de la protección de la intimidad frente a la actividad y creciente poder de las bases de datos, constituye la concreción legislativa de esta nueva concepción.

3. El derecho a la intimidad como pretensión de transparencia del accionar del banco de datos: «El derecho a no ser discriminado».

En las elaboraciones doctrinales más recientes se sostiene por el jurista Stefano RODOTA que «el problema no consiste en garantizar la opacidad de la vida privada sino la transparencia del accionar de entidades públicas y privadas». Este autor considera que la privacidad en su nueva configuración no es el derecho a ser dejado sólo ni el nuevo derecho a supervisar a quienes poseen información, sino que es, fundamentalmente, el «derecho a no ser discriminado» [5].

De modo muy sutil, a través de la informática y de la combinación y entrecruzamiento de datos, se pueden afectar los derechos y libertades mediante las informaciones llamadas sensibles o nominativas (referentes a convicciones o creencias religiosas, o políticas, origen racial, hábitos, costumbres, ideología, etc.), que pueden conducir a tratamientos discriminatorios, respecto de los particulares involucrados, por parte de quienes detenten la información. De allí que este reclamo integre hoy el elenco de exigencias para una adecuada tutela de la privacidad.

III. BASES DE DATOS, PRIVACIDAD Y RESPONSABILIDAD CIVIL EN EL DERECHO ARGENTINO

En el derecho privado argentino no existe, de lege data, un marco legal que, en forma específica, regule el derecho a la privacidad con relación al tratamiento automatizado de datos personales por las bases de datos. Sin embargo, se cuenta con el art. 1071 bis del Código Civil según el cual el que arbitrariamente se entrometiere en la vida ajena ... perturbando de algún modo su intimidad y el hecho no fuere un delito penal será obligado a cesar en tales actividades, si antes no hubieren cesado y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias...». Este artículo (que tiene su raigambre fundamental en el art. 19 de la Constitución

[4] ROPPO, ENZO, «Informaticca, tutela della privacy o diritti di liberta», en ALPA, G., Diritto dell' informatica, Giuffre, 1985, n.º 4, pp. 22-23.

[5] CORREA, C. y Otros, «Derecho Informático», Buenos Aires, *Depalma,* 1987, p. 250.

Nacional) en cuanto sanciona al «que arbitrariamente se entrometiere en la vida ajena»... «perturbando de cualquier modo su intimidad» permite, en una interpretación amplia, incluir la recolección o difusión de datos personales por parte de la base de datos, entre los modos de perturbar la intimidad.

Aplicando este artículo al problema de la actividad informática intrusiva, la Comisión N.º 1 del «I Congreso Internacional de Derecho de Daños en honor del Dr. Jorge Mosset Iturraspe» (Bs. As., abril de 1989), se pronunció, entre otras conclusiones, en el sentido de que «Toda intromisión se presume ilegítima, salvo que medie una causa de justificación» y que «la mera intromisión o amenaza de intromisión, independientemente de que haya menoscabo patrimonial o moral y de que el agente haya obrado con dolo o culpa autoriza el ejercicio de las siguientes acciones: acción de cese o abstención, acción de inhibición. Estas acciones deben ser tratadas con criterio amplio, precaucional y expeditivo» [6].

Además, en diversas jornadas y congresos se han reconocido los derechos de la persona a controlar sus datos, exigiendo su rectificación o cancelación como también que sean utilizados para el fin para el cual fueron recogidos y que la intromisión da lugar al resarcimiento de los daños materiales y morales que se hubieran producido, siendo aplicables los principios generales de la responsabilidad civil [7].

En lo que respecta a esta cuestión, cabe sostener que en el derecho privado argentino la responsabilidad de la base de datos por la intrusión a la intimidad es de naturaleza objetiva, fundada en el riesgo o la garantía y que encuentra su régimen legal en el art. 1113-2.º párr. 2.ª parte del Codigo Civil que regula los daños causados por el riesgo o vicio de las cosas.

En efecto: La manipulación de datos sensibles o nominativos que puede tener lugar en la base de datos, donde éstos se analizan, se combinan, se reagrupan, y se pueden distorsionar, etc., determina que esta actividad se deba catalogar como riesgosa, dado que todos esos actos son posibilitantes de daños. Es la naturaleza sistemática del banco de datos la que torna peligrosa su actividad y la que, a su vez, le impone un severo deber de seguridad en el cuidado de la información tratada.

Así lo sostuvo el Prof. Jorge MOSSET ITURRASPE en las XI Jornadas Nacionales de Derecho Civil, expresando que «Debe calificarse como riesgosa o peligrosa la actividad de registración de informaciones nominativas relativas a los orígenes raciales, opiniones políticas, filosóficas o religiosas, o relacionadas con la intimidad de las personas».

De la concordancia de los arts. 1071 y 1113 del Código Civil argentino resulta que estamos frente a un supuesto de responsabilidad objetiva tanto

---

[6] MOSSET ITURRASPE, J. y OTROS, *«Daños»*. Buenos Aires, *Depalma,* 1991. p. 66.

[7] ZANNONI, E., El daño en la responsabilidad civil, 2a. ed., Buenos Aires, *Astrea,* 1987, p. 390.

por el carácter riesgoso de la actividad del banco de datos como porque el deber de resarcir obedece a la intrusión a la intimidad no justificada. Se responde de las consecuencias inmediatas y mediatas, excluídas las casuales y las remotas. Además, tratándose de responsabilidad objetiva, cabe prescindir de la cuestión referente a si el damnificado se encuentra unido contractualmente o no a la base de datos, por cuanto ello resulta indiferente, en razón de que «quien está incurso en una responsabilidad objetiva no comete un acto ilícito sino que practica una actividad lícita, a la cual, sin embargo, pese a esa licitud, la ley ha vinculado la obligación de resarcir los perjuicios derivados de ella» [8].

La lesión de la intimidad, o privacidad, constituye un supuesto de daño moral, dado el carácter no patrimonial de los derechos de la personalidad.

De modo que, si ha habido una intrusión a la intimidad del sujeto, perturbándola de cualquier modo, y esa intrusión produce daños patrimoniales (indirectos), la base de datos incurre en responsabilidad, siéndole aplicable el régimen del Código relativo a las cosas, entre las que quedan comprendidas las actividades riesgosas por su naturaleza o por las circunstancias de su realización. «La responsabilidad existe por el sólo hecho de causación del daño en el ejercicio de la actividad peligrosa o del uso de la cosa con riesgo. Es como si la ley dijera a los responsables: están autorizados a la actividad o al uso peligrosos, pero en todo caso a propio riesgo» [9].

IV. CONCLUSIONES

1. El derecho a la privacidad, «derecho de intimidad», «derecho sobre la propia esfera de secreto» es un derecho de la personalidad que actualmente consiste no sólo en el derecho del individuo a no sufrir perturbaciones en su zona espiritual íntima (identidad, personalidad moral, ideología, imagen, secreto de su vida particular, situación patrimonial) y a vedar el uso de información sobre sí mismo, sino también en la facultad de controlar y lograr que de esta información no se haga un uso impropio, fundamentalmente por las potentes bases de datos del mundo moderno.

2. Acorde al carácter no patrimonial de los derechos de la personalidad, la lesión de la intimidad o privacidad constituye un supuesto de daño moral.

3. El uso incorrecto, desviado o abusivo de información nominativa puede además configurar responsabilidad civil si por la intrusión arbitraria a la intimidad se le causaran al afectado daños patrimoniales (indirectos). En este caso se aplican las normas generales de la responsabilidad civil, siendo objetivo el factor de atribución de responsabilidad y fundado en el riesgo o la garantía.

---

[8] LLAMBIAS, J. J., «Responsabilidad objetiva: daños me diatos y daño moral», *La Ley*, 1980, D, 81.

[9] ORGAZ, A. «La Culpa», Buenos Aires, *Depalma,* 1970, n.º 75.

4. En el derecho privado argentino la ilicitud genérica surge del art. 1113 del Código Civil (régimen de los daños causados por las cosas) y la específica resulta del art. 1071 bis de dicho Código, según el cual «el que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación».

La transparencia de las bases de datos como mecanismo de protección de la intimidad de las personas

MANUEL SÁNCHEZ DE DIEGO FDEZ. DE LA RIVA

Dpto. de Derecho Constitucional (Derecho de la Información)
Facultad de Ciencias de la Información.
Universidad Complutense de Madrid
(ESPAÑA)

La informática constituye un instrumento que permite multiplicar de forma asombrosa las capacidades del hombre y, por tanto, de incrementar sus potencialidades. El tratamiento automatizado de todo tipo de datos permite que las acciones del hombre sean más eficaces con menos medios. En palabras de ALVAREZ-CIENFUEGOS: «La información, de la índole que sea, se ha convertido en un bien jurídico de extraordinario valor. No sólo mueve intereses económicos importantes sino que, también, constituye un elemento imprescindible para el desarrollo de múltiples iniciativas públicas y privadas» [1].

En cuanto instrumento, la informática es susceptible de una utilización contraria al propio ser humano y, en concreto, se ha convertido en un peligroso medio que permite violar de forma *cuasi impune* la intimidad de las personas a través de una manipulación informática de los datos personales. Una primera solución consistiría en establecer normas jurídicas que confor-

[1] ALVAREZ-CIENFUEGOS SUÁREZ, J. M.: «El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los bancos de datos» en Davara, M. A. y otros «Encuentros sobre Informática y Derecho 1990-1991». *Universidad Pontificia de Comillas-Aranzadi* 1992. Página 18.

masen sistemas informáticos cerrados sólo accesibles a personas autorizadas expresamente para ello[2].

Sin embargo, la información es poder y si se veta el acceso de los ciudadanos a los medios informáticos y sus recursos, se crearán situaciones de desigualdad e incluso de alienación. En palabras de PÉREZ LUÑO referidas a nuestro días: «contemporáneamente se produce una agresión a la igualdad, más implacable que en cualquier otro período histórico, desde el momento que se desarrolla una profunda disparidad entre quienes poseen, o tienen acceso, al poder informático y quienes se hallan marginados de su disfrute» [3].

Ante esta situación se deben buscar mecanismos técnicos, educacionales, jurídicos y de todo tipo que permitan un adecuado aprovechamiento de los recursos informáticos sin que por ello la igualdad y la libertad se vean burladas.

En España nos encontramos inmersos en un proceso de creación normativa importante: se trata de desarrollar la protección de la intimidad de las personas frente al tratamiento automatizado de datos personales. Como primera aproximación nos vamos a referir al **derecho a la intimidad informática** [4] como derecho humano recogido en la Constitución española. Como segundo punto de reflexión realizaremos una serie de consideraciones sobre

---

[2] Tal y como ocurrió en la antigüedad con los llamados *Libri Sibyllini* celosamente guardados en el templo de Júpiter Capitolino por los *duoviri sacris faciundis* por dichos libros contener los destinos del pueblo romano. Véase FARIAS GARCÍA, P. «Libertades Públicas e información». *EUDEMA*. Madrid, 1988. Página 49 y más específicamente GIL, L.: «La censura en el mundo antiguo» *Alianza Universidad*. Madrid, 1985. Páginas 98-99.

[3] PÉREZ LUÑO, A. E.: «Del *Habeas Corpus* al *Habeas Data*» en Davara, M. A. y otros «Encuentros sobre Informática y Derecho 1990-1991» *Universidad Pontificia de Comillas-Aranzadi* 1992. Página 175.

[4] Se han empleado los términos «derecho a la autoderminación informativa» (LUCAS MURILLO, P.: «El derecho a la autodeterminación informativa». Madrid 1990) como traducción de *Recht auf informationelle Selbstbestimmung* o, también «derecho a la autoderminación informática» para referirse a la protección del individuo contra la recogida, el almacenamiento, la utilización, la transmisión y, en su caso, la difusión de datos concernientes a una persona por medios automatizados. Sin embargo, la expresión «derecho a la autodeterminación» tiene en la actualidad, tanto en el derecho internacional como constitucional, y a nivel general una significación muy precisa –referida a la capacidad de los pueblos a determinar su destino político– y totalmente diferente a la que se le quiere dar.

De igual forma referirnos a una «libertad informática (FROSINI: «Il diritto alla riservatezza come diritto di libertà». Milano, 1985. Pág. 26 PÉREZ LUÑO, A.: «Derechos humanos, Estado de Derecho y Constitución». Madrid, 1984. Pág. 370. PÉREZ LUÑO, A.: «Concepto y concepción de los derechos humanos». Doxa, núm. 4. 1987. HERRERO-TEJEDOR, F.: «Honor, intimidad y propia imagen». Madrid, 1990. Página 40) puede plantear una idea errónea sobre su significado, pues tal expresión parece apuntar a la capacidad para acceder a la informática.

Es por todo ello que proponemos el término de **derecho a la intimidad informática**. Cierto que esta expresión no facilita la diferenciación con el derecho a la intimidad (esta es la razón que utiliza LUCAS MURILLO para optar por «derecho a la autodeterminación informativa». Ob. cit. pág. 124) y que ello puede suponer un problema a la hora de configurar como autónomo este derecho. Sin embargo, una vez establecida la independencia del derecho a la intimidad informática respecto del derecho a la intimidad, la expresión «derecho a la intimidad informática» creemos que es el más adecuado porque expresa el origen de este derecho y no induce a confusión con otros derechos totalmente distintos.

el proyecto de *Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal* (LORTAD).

La necesaria transparencia de los archivos administrativos será la tercera cuestión a tratar, para finalizar con una argumentación a favor de dicha transparencia como mecanismo de protección, aunque pueda parecer paradójico, de la intimidad de las personas.

I. EL DERECHO A LA INTIMIDAD INFORMATICA

Determinados datos privados son protegidos jurídicamente frente a la curiosidad de terceros o de los poderes públicos por el derecho a la intimidad. En ellos la naturaleza íntima del dato es la razón de tal protección.

Cuando nos referimos al **derecho a la intimidad informática** la protección de los datos de carácter privado no se realiza por la naturaleza más o menos íntima de los datos, sino por el hecho que esos datos van a ser procesados de forma automática [5]. La posibilidad técnica de procesar muchos datos en principio inofensivos, esto es, no sensibles a la intimidad, y de obtener una «radiografía» moral, política, social o, incluso, psicológica de una persona concreta, ha supuesto el desarrollo de un derecho a la intimidad informática. El derecho a la intimidad informática hunde sus raíces en el derecho a la intimidad [6], ahora bien, presenta varias peculiaridades respecto a este derecho fundamental. Tras este derecho humano se encuentra la idea que la información es poder y la utilización incontrolada de ese poder genera quiebras importantes de los principios de libertad e igualdad, comenzando por los derechos a la intimidad y el honor [7].

La Constitución española siguiendo la línea de las constituciones más avanzadas [8] recogió este derecho a la intimidad informática, y lo hizo en un

---

[5] En el mismo sentido LUCAS MURILLO: «No se reduce, por otra parte, a tutelar las que podríamos considerar informaciones "sensibles", ni a las relativas a los aspectos recónditos de la vida del individuo. Al contrario, tendremos la ocasión de ver cómo se extiende a datos de apariencia, en principio, inocua y que, en modo alguno, se sitúan en esa esfera privada en sentido estricto que cada uno reserva exclusivamente para sí» (LUCAS MURILLO, P.: Ob. cit., pág. 26).

[6] Cierto que al tratar del derecho a la intimidad se ha producido una *inflación* en su contenido que dificulta su definición (Véase DESANTES GUANTES, J. M. Y SORIA, C.: «Los límites de la información». Asociación de la Prensa de Madrid, 1991. Página 107 y siguientes).

[7] En este sentido PÉREZ LUÑO manifiesta: «en una sociedad como la que nos toca vivir en la que la información es poder y en la que ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario» (PÉREZ LUÑO, A. E.: *«Del Habeas Corpus al Habeas Data»* Ob. cit. página 175).

[8] La Constitución Portuguesa de 1975 recogió en su artículo 35 el derecho a la intimidad informática:

Utilizaçao da informatica.

1. Todos os ciudadâos têm o direito de tomar conhecimiento do que constar de regitos mecanográficos a seu respeito e do fim a que se destinam as informaçoes, podendo exigir a rectificaçao dos datos e a sua actulizaçao.

2. A informatica nâo pode ser usada para tratamento de datos referenteds a convicçoes

apartado del precepto que comienza garantizando el derecho al honor, a la intimidad, y a la propia imagen [9]. En concreto el artículo 18 establece en su apartado 4.º:

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Esta Ley que menciona el artículo 18.4, en virtud del artículo 81 de la Constitución española deberá tener el rango de Ley Orgánica [10] y respetar el

---

políticas, fé religiosa ous vida privada, salvo quando se trate do procesasamento de datos nâo identificáveis para fins estadísticos.

3. E proibida a atribuiçao de un mero único ais ciudadâos.

Como puede observarse esta disposición portuguesa, mucho más precisa que la española, prohíbe en su párrafo 3.º de forma taxativa el número de identificación único –que en España es casi una realidad gracias al DNI/NIF–; establece en su párrafo 2.º de forma flexible –al permitir su tratamiento anónimo para fines estadísticos– pero a la vez eficaz, una protección de los llamados datos sensibles y, por último, menciona de forma clara las facultades de acceso a los datos, de conocimiento de los fines de la base de datos y de rectificación de datos por parte de los afectados.

En 1978 el Land de Renania del Norte-Westfalia (Alemania) modificó su artículo 4.º reconociendo un derecho fundamental a la protección de datos. Estados norteamericanos como Alaska, Arizona, California, Florida, Iowa, Montana, Ohio, o Washington han modificado sus constituciones para reconocer derechos sobre la intimidad informática.

Entre las disposiciones legales sobre esta materia podemos citar la ley de protección de datos (*Datenschutzgesetz*) del land de Hesse (Alemania) de 7 de octubre de 1970, el *Fair Reporting Act 1970* norteamericano de 26 de octubre de 1970, la Ley sueca de 11 de mayo de 1973, la Ley federal alemanana de 27 de enero de 1977, la Ley húngara de 27 de enero de 1981... (Véase AUDIJE PACHECO, CAMPUZANO ROBLEDO, FERNÁNDEZ MUGUELLES y RUBIO SIERRA: «Consideraciones acerca de una futura Ley española para limitar el uso de la informática», en III Encuentro sobre la informática en las Facultades de Derecho (Mayo 1989). Madrid 1990. Páginas 214 a 222. Así como MINISTERIO PARA LAS ADMINISTRACIONES PUBLICAS, Dirección General de Organización, Puestos de Trabajo e Informática: «Leyes de protección de datos». Madrid, 1988 y ARAMENDI, CABELLERO, DOMAICA, MÉNDEZ, PENADES y VALLÉS: «Leyes de protección de datos», en II Encuentro sobre la informática en las Facultades de Derecho (Mayo 1988). Universidad Pontificia de Comillas. Madrid. Páginas 59 y siguientes.

[9] El artículo 18 establece:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Realmente no se puede decir que el párrafo 1.º se refiera a un único derecho, sino de tres íntimamente conectados. Véase como referencia la diferenciación y conexión entre el derecho a la propia imagen y el derecho a la intimidad en AMAT LLARI, Eulalia: «El derecho a la propia imagen y su valor publicitario». *Edt. La Ley*. Madrid, 1992.

Los apartados segundo y tercero se refieren a aspectos concretos del derecho a la intimidad, mientras que el cuarto, que consideramos como el arranque del derecho a la intimidad informática tiene una entidad propia, incluso cuando hace referencia no sólo al derecho a la intimidad, sino también a otros derechos.

[10] Exigencia de Ley Orgánica en el que está de acuerdo la mayoría de la doctrina. Véase LUCAS MURILLO: Ob. cit. páginas 175 a 178.

contenido esencial del derecho, tal y como exige el artículo 53.1 de la Norma Fundamental [11].

Por encontrarse recogido dentro de la sección 1.ª del capítulo 2.º del Título I, el derecho a la intimidad informática es un derecho fundamental de los especialmente protegidos. Así mismo por tratarse la Constitución de una norma de aplicación directa, este derecho fundamental puede ser invocado ante los órganos de justicia sin necesidad de esperar a la norma que lo desarrolle.

Trataremos de fijar el contenido esencial [12] del derecho a la intimidad informática. LUCAS MURILLO al referirse al contenido de este derecho entiende que está integrado «por las diferentes facultades que se le reconocen (al individuo) para controlar el uso de información personal que le atañe tanto en el momento de la recogida de los datos, cuanto en el de su tratamiento y conservación, como, en fin, en el de la transmisión» [13]. En este sentido, el contenido esencial del derecho a la intimidad informática consistirá en el **derecho de toda persona a controlar sus datos de carácter personal tratados informáticamente.** Este contenido esencial supone un control sobre la «colecta de información», o mejor dicho, la recogida de datos para ser introducidos en un sistema informático; sobre el «tratamiento automatizado» de los datos –que supone «registro de los datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado o extracción» [14]–, la

---

El artículo 81 de la Constitución establece:

Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.

La aprobación, modificación o derogación de las leyes orgánicas exigirá mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto.

[11] Artículo 53.1 de la Constitución:

Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el Artículo 161, 1 a).

[12] La sentencia del Tribunal Constitucional de 16 de noviembre de 1981 (BOE 28 de noviembre) nos explica que:

«Se entiende por contenido esencial aquella parte del contenido de un derecho sin la cual éste pierde su peculiaridad, o, dicho de otro modo, lo que hace que sea recognoscible como derecho perteneciente a un determinado tipo. Es también aquella parte de contenido que es ineludiblemente necesaria para que el derecho permita a su titular la satisfacción de aquellos intereses para cuya consecuencia el derecho se otorga...».

[13] LUCAS MURILLO, P.: Ob. cit. Página 185.

[14] En el artículo 2.c) del «Convenio para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal», se define a efectos del propio Convenio, el término «tratamiento automatizado» como

las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión

Realmente la «difusión» de la información obtenida gracias a los ordenadores, no supone algo propio del tratamiento automatizado, se trata de algo posterior a la recuperación –extracción en términos del Convenio–. En este sentido no estamos de acuerdo con la inclusión de la difusión en la definición de «tratamiento automatizado». Debía de haberse excluido, al igual que entiende

reproducción o difusión de los datos de carácter personal o de los resultados obtenidos a partir de ellos y, por último, ese control exige que el sujeto pueda tener conocimiento de las bases de datos en donde pudieran figurar sus datos personales y pueda acceder a sus datos.

Así pues, entendemos que el derecho a la intimidad informática se proyecta sobre los tres momentos claves por los que circulan los datos de carácter personal: el momento previo a ser introducidos en un ordenador, esto es, la captura o recogida de la información; una vez que se encuentran los datos dentro del sistema informático (todo lo referente a la conservación y tratamiento automatizado de los datos) y; en tercer lugar, la difusión de los datos después de ser recuperados.

Comenzando por este último aspecto del derecho a la intimidad informática hemos de manifestar que la facultad de la persona de controlar los datos cuando se trasmiten desde el sistema informático tiene una doble perspectiva. Por un lado, la difusión de los datos y toda su problemática se reconduce al tradicional derecho a la intimidad o en su caso al derecho al honor, incluso en aquellas informaciones que haya proporcionado el sistema informático a resultas de un cruce de datos (piénsese en el perfil psicológico de una persona, o la valoración sobre la reputación profesional y ética de un empresario...). Por otro lado, es importante señalar la posibilidad que tiene la persona afectada de conocer a quienes le han sido trasmitidos sus datos y qué finalidad persigue el que recibe los datos.

El problema que se plantea relacionado con el control de los datos ya introducidos en el sistema informático es el más complejo. A este asunto la doctrina ha dedicado un especial interés y se ha permitido configurar un llamado *habeas data* [15] que PÉREZ LUÑO define como «la facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos de datos informatizados» [16]. Podría desglosar este derecho en las facultades de cualquier persona de:

---

la Memoria Explicativa del Convenio que se hizo con la «colecta de información», acción que no se considera propia del «tratamiento automatizado», aunque una interpretación del precepto 2.c en relación con el 5.c permitiría incluirla en la expresión «registro de datos».

Unicamente cabría incluir la «difusión» dentro del «tratamiento automatizado» cuando se entienda como transmisión de datos dentro de un sistema informático –transferencias de datos entre ficheros, de ficheros entre soportes físicos (de diskettes a discos duros, de discos duros a cintas...)– o entre sistemas informáticos –transferencia de datos entre ordenadores–. Dicho de otra forma, podemos utilizar un concepto estricto de «tratamiento automatizado» que no incluya ni la difusión, ni la captación de datos; uno mucho más amplio que sí que abarque tales acciones y; por último, entender, como hace el Convenio, que el «tratamiento automatizado» incluye la difusión de datos y no la captación.

Lo importante es entender que el derecho a la intimidad informática abarca tanto la captación de datos, el procesamiento y la reproducción de los mismos.

[15] PÉREZ LUÑO, A. E.: «*Del Habeas Corpus* al *Habeas Data*» Ob. cit. Páginas 173 y siguientes.

[16] Ibidem. Página 175.

*conocer la existencia de bases de datos –fichero automatizado– y las características de la mismas –finalidad, con que otras bases de datos se cruza información...– en donde pudieran figurar datos personales propios.

*conocer la información que en una base de datos exista a cerca de él.

*poder rectificar la información errónea o inapropiada que le afecte.

*recurrir a la autoridad competente, incluso a la vía judicial, en el caso de serle impedido la realización de alguna de las anteriores facultades.

De los tres momentos sobre los que se proyecta el derecho a la intimidad informática es el previo, el que corresponde a la captación de datos, en donde la protección a la intimidad informática parece más fácil.

A la vista del «Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal» podemos preguntarnos si el derecho a la intimidad informática protege al particular también en el momento de la captación de datos. El punto 31 de la memoria explicativa de dicho convenio entiende que la colecta de información queda fuera de la noción de «tratamiento automatizado». Esta interpretación no impide que el Convenio contemple la colecta de datos [17] y la necesidad de establecer un control sobre la misma. En concreto, el artículo 12 en el caso de flujo transfronterizo de datos se refiere también a los «datos de carácter personal que sean objeto de un tratamiento automatizado o **reunidos con el fin de someterlos a ese tratamiento**». Más explícito es el artículo 5 del Convenio que establece:

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

El proyecto de Ley Orgánica, del que a continuación nos ocuparemos, despeja múltiples dudas, entre ellas ésta, al establecer mecanismos de limitación en la recogida de datos para su tratamiento informático.

II. EL DESARROLLO DE LA INTIMIDAD INFORMATICA: EL POR QUE DE LA LORTAD

El mandato constitucional del artículo 18.4 aparenta ser la razón que ha movido al Gobierno a enviar un proyecto de Ley Orgánica a las Cortes Españo-

[17] Observamos que no existe una adecuación entre el nombre del Convenio –designado como «para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal»–, su contenido y el derecho a la intimidad informática. Y no solamente porque en el Convenio se trate de forma accesoria la captura de datos no considerándola parte del «tratamiento automatizado», sino también porque el propio Convenio prevé que los países signatarios extiendan la protección prevista a los datos personales no tratados automáticamente.

las. Sin embargo, **el por qué se legisla en este momento y no antes parece que obedece más a la necesidad de adecuar nuestra normativa a la propia de los países comunitarios, que a la existencia de una sensibilidad del Ejecutivo español respecto del derecho a la intimidad informática**.

Varias son las razones que nos hacen sospechar esa falta de sensibilidad, comenzando por el retraso en enviar el proyecto de Ley al Congreso de los Diputados. Hemos tenido que esperar casi 13 años desde que en 1978 la Constitución estableció la obligación de legislar sobre el tema. Y de esa inacción es primer responsable el Gobierno después que el 22 de marzo de 1987, hace casi cinco años, se hubo aprobado en el Congreso de los Diputados una moción del Grupo Parlamentario Socialista instando al Gobierno a enviar el correspondiente proyecto de Ley. Además, ante las proposiciones de Ley sobre protección de datos del Grupo Parlamentario Popular (2-IV-1987) y de Izquierda Unida-Ezquerra Catalana (16-VI-1988), la mayoría que sostiene al Gobierno decidió en ambos casos esperar el proyecto de Ley del Ejecutivo. Cierto que la firma de el *Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* obligó de alguna forma a tomar medidas que se plasmaron en una provisional e insuficiente disposición transitoria primera de la *Ley Orgánica 1/82, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen* –norma tristemente famosa porque ha servido para solicitar a los medios de comunicación millonarias cifras como indemnizaciones–. Dicha disposición establece que:

«en tanto no se promulgue la normativa prevista en el artículo 18, apartado 4 de la Constitución, la protección civil del honor, la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se desarrollarán por la presente ley.»

La falta de sensibilidad del Ejecutivo procede no sólo del retraso en regular el derecho a la intimidad informática o del bloqueo sistemático de las proposiciones de Ley de la oposición, también se aprecia en la redacción del proyecto de LORTAD. Norma que si es importante su aparición, resulta bastante insatisfactoria en varios extremos.

La posibilidad de transmisión de datos más allá de las fronteras, el llamado flujo transfronterizo de datos, es en última instancia la causa del proyecto de Ley que nos ocupa. A nivel internacional –comenzando por el artículo 12 del ya mencionado Convenio Europeo número 108– se exige que para el libre flujo transfronterizo de datos, el país de destino cuente con un sistema de protección de datos equivalente al del país de origen de los datos. La falta en España de eficaz sistema de protección de datos adecuado significaría la exclusión de nuestro país de un espacio uniforme, en donde el libre flujo de datos «constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial

internacional pueden ser simples botones de muestra» [18]. Coherente con esta idea el propio proyecto de Ley Orgánica dedica un título al «Movimiento internacional de datos» -artículos 32 y 33– en donde como principio general se establece que «no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal...con destino a países que no proporcionen un nivel de protección equiparable al que preste la presente Ley...».

De alguna forma si tenemos presente el porqué se legisla sobre la protección de datos de carácter personal podremos entender mejor cuáles son los principios que inspiran dicha norma y qué aspectos de dicha norma nacen deficientes. En concreto, esto nos permitirá entender la carencia de un principio de transparencia general de los ficheros automatizados en el proyecto de LORTAD y por qué no ha afrontado cuestiones directamente relacionadas como la regulación del acceso de los ciudadanos a los archivos administrativos –artículo 105 b) de la Constitución española–.

III. ALGUNAS DE LAS IDEAS QUE SUBYACEN EN LA LORTAD

La parte de la vida humana que la LORTAD viene a proteger se encuentra en el ámbito privado. Es la **privacidad** el objeto de este proyecto de Ley. Así se reconoce en la propia exposición de motivos del proyecto de Ley:

«El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de privacidad, y no de intimidad: aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de las personas –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo– la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. ...»

El hecho que la privacidad del individuo sea el objeto de protección del proyecto de Ley Orgánica que nos ocupa, ha suscitado la pregunta de si al no estar el derecho a la privacidad expresamente recogido en la Constitución Española, no es preciso que la protección de este derecho se realice mediante una Ley Orgánica, bastando para ello una simple Ley ordinaria.

Esta cuestión, a nuestro juicio, ha de ser resuelta negando tal posibilidad. Entendemos, tal y como antes hemos sostenido, que es preciso una regulación mediante Ley Orgánica. Es cierto que el proyecto de LORTAD se ocupa de

[18] Párrafo segundo del apartado IV de la exposición de motivos del proyecto de *Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).*

los datos privados de las personas y no únicamente de los datos íntimos. Pero, y esto es lo importante, el hecho es que el tratamiento automatizado de esos datos personales, privados aunque no íntimos, permite el conocimiento de la intimidad de la persona. De ahí que en último término el objeto de protección de la LORTAD, diga lo que diga su exposición de motivos, es el derecho a la intimidad. Es más, se protege la intimidad frente a las agresiones provenientes de los sistemas informáticos capaces de almacenar, procesar, generar y proporcionar datos de las personas. De ahí la denominación escogida de **derecho a la intimidad informática** en tanto en cuanto que la protección no se limita a los datos íntimos o los sensibles, sino también a los privados; por lo que dicho derecho tiene un principio diferenciador con el simple derecho a la intimidad.

En segundo lugar observamos que la protección se realiza desde mecanismos cautelares, tal y como establece la propia exposición de motivos:

«La ley está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones...»

Pese a que esto es cierto, también lo es que el proyecto de LORTAD establece importantes mecanismo de control *a posteriori*, en especial una Agencia de Protección de Datos [19] encargada de velar por el cumplimiento de las disposiciones de la LORTAD y todo un título VII dedicado a infracciones y sanciones de carácter administrativo que pueden llegar a ser de 100 millones de pesetas. Pero tanto de una forma como de otra, **la protección se realiza mediante un control restrictivo de los datos**. Se trata de buscar la seguridad de la información mediante el hermetismo de las bases de datos, de forma que sólo determinados sujetos puedan manejar informáticamente los datos personales cuando se cumplen determinadas circunstancias y, casi excepcionalmente, los afectados pueden conocer y controlar las informaciones que les conciernen procesadas en bases de datos informatizadas [20].

En tercer lugar, debemos de entender que la LORTAD pese a nacer con vocación de regular en general todos los ficheros automatizados de datos personales [21], en su propio articulado, comenzando por el artículo 2, nos

---

[19] Cuyo éxito dependerá no sólo de la independencia con que se configure dicho órgano del Poder Ejecutivo, sino también de los medios materiales de los que disponga.

[20] Sobre la incidencia de la LORTAD en un sector económico como es el del marketing directo podemos recoger las manifestaciones de la representante de la Asociación Española de Marketing Directo en la Comisión de Libertades e Informática: «Los ficheros informáticos son el activo más importante de una empresa de Marketing Directo ... desearíamos hacer hincapié en la absoluta necesidad de una ley de protección de datos positiva y abierta, destinada a prevenir únicamente las actitudes dictadas por la mala fe,y el enorme desatino que supone un modelo legislativo como la LORTAD, cuyo fracaso se ha hecho manifiesto en otros países...» (SÁNCHEZ, E.: «El Marketing Directo y la Protección de Datos» en revista NOVATICA volumen XVIII núm. 96. Marzo-abril, 1992. Página 73).

[21] Por datos personales hemos de entender aquellos concernientes a personas físicas que se encuentran identificadas por el sistema informático.

encontramos múltiples exclusiones, tanto para aquellas bases de datos para los que no se aplica de forma absoluta o relativa la LORTAD –artículo 2.2 [22]–, como para los ficheros que reciben una regulación específica –artículo 2.3 [23]–. Existen también diversas excepciones que afectan a cuestiones importantes como el consentimiento del afectado a efectos del tratamiento de sus datos personales. Consentimiento que no se exige en un gran número de situaciones –artículo 6.2 [24]–. Así pues, se trata de norma jurídica con demasiadas excepciones en su ámbito de aplicación, en definitiva una norma que **regula solo parcialmente a los ficheros automatizados** de datos personales y que para nada desarrolla el derecho de los ciudadanos a la información.

En cuarto lugar, podemos observar que el **tratamiento diferenciado entre ficheros de titularidad pública y ficheros de titularidad privada,** tal y como se reconoce en la propia exposición de motivos:

...ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que los de titularidad pública.

---

[22] En concreto el artículo 2.2 del proyecto de LORTAD establece:

El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:

a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales.

c) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.

e) A los ficheros mantenidos por los Partidos Políticos, Sindicatos e Iglesia, Confesiones y Comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y exmiembros sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

Nota: figura en subrayado las modificaciones introducidas en la Comisión Constitucional al aceptarse la enmienda 161 del CDS.

[23] Tal y como establece el artículo 2.3 de la LORTAD:

Se regirán por disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los sometidos a la normativa sobre protección de materias clasificadas.

c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.

d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjucio de lo dispuesto en el artículo treinta y seis.

e) Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional.

[24] A tenor del artículo 6 del proyecto de LORTAD:

1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos del carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para un mantenimiento de las relaciones o para el cumplimiento del contrato.

Sin embargo, un principio que debería parecer sencillo como es el de publicidad de las acciones la Administración y, por ende, la transparencia de sus actuaciones y de los ficheros públicos, no se recoge en ninguna parte del articulado de la LORTAD.

En efecto, es cierto que un particular teme las posibles agresiones a su intimidad producidas por sistemas informáticos del Banco X, la Aseguradora Y, la empresa de marketing directo JJ o en general de cualquier fichero de titularidad privada; sin embargo, lo que preocupa de verdad al ciudadano es la agresión informática que puede sufrir por parte del Estado. La idea del *Hermano Grande* del que hablaba Orwell [25] que nos vigila es la que realmente inquieta. Hoy en día con el NIF, DNI, Carnet de Conducir... [26] el número de identificación único parece ser una realidad en nuestro país que permite el fácil cruce de datos.

Es positivo que se desarrolle el artículo 18.4 y se establezcan mecanismos de protección del derecho a la intimidad informática. Sin embargo, la LORTAD podía haber sido aprovechada para establecer fórmulas de acceso de los ciudadanos a las bases de datos públicas. Ello conllevaría no sólo una mayor transparencia de la acción administrativa, sino también una protección añadida al derecho a la intimidad informática tal y como trataremos de demostrar.

IV. LA TRANSPARENCIA DE LA ACCION ADMINISTRATIVA

Tradicionalmente en la mayoría de los países se ha mantenido **el principio de confidencialidad de los documentos administrativos.** «Este principio ha sido progresivamente contestado, solicitándose desde diversas instancias sociales una inversión del sistema, mediante la conversión en regla del acceso a tales documentos, quedando la confidencialidad como excepción», tal y como manifiesta SOUVIRON MORENILLA [27].

La aparición dentro del título IV –«Del Gobierno y de la Administración»– del artículo 105 b)[28] de la Constitución Española ha supuesto un importante paso adelante en favor de los ciudadanos, aunque hemos de confesar que existe una importante división de la doctrina sobre el significado y

---

[25] ORWELL, G.: «1984».

[26] Sobre la implementación en nuestro país del NIF, mediante el artículo 113 de la Ley de Presupuestos Generales del Estado para el año 1988, sus antecedentes y enjuiciamiento véase BELLO PAREDES, Santiago A.: «El Número de Identificación Fiscal, algunas consecuencias de su incardinación en nuestro ordenamiento jurídico» en Davara, M. A. «Encuentro sobre Informática y Derecho 1990-1991. *Universidad Pontificia de Comillas-Aranzadi* 1992. Páginas 160 a 170.

[27] SOUVIRON MORENILLA, J. M.: «Notas para una Ley sobre la información». Presidencia de Gobierno, Madrid, 1980. Página 36.

[28] Este precepto pasó prácticamente desapercibido en las discusiones parlamentarias, aprobándose prácticamente la redacción original del entonces artículo 103 b) del anteproyecto de Constitución. Véanse la edición de las CORTES ESPAÑOLAS: «Constitución española. Trabajos parlamentarios». Madrid, 1980.

contenido de dicho precepto [29]; así como una interpretación de la Sala 3ª del Tribunal Supremo de fecha 16 de octubre de 1979 [30] que niega la eficacia inmediata del artículo 105 b) y afirma su mero carácter programático [31].

El mencionado artículo 105 establece en su párrafo b que la Ley regulará [32]:

El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas

A la pregunta de si consagra el artículo 105 b) un derecho fundamental ha respondido DE LA OLIVA que «no consagra este precepto, desde luego, un derecho fundamental, puesto que si la facultad de acceder a archivos y registros se estimase comprendida en el derecho a obtener o recibir información, tal derecho surgiría **ex** artículo 20, como lo entienden por ejemplo MUÑOZ MACHADO y SAINZ MORENO» [33]. Sin embargo, DESANTES aboga por su reconocimiento como derecho fundamental [34] al entender que el artículo 105 b) se refiere al derecho a la documentación [35] y que dicho derecho se inscribe en el derecho a la información. Al respecto DESANTES manifiesta: «el derecho del artículo 105 b) no es otra cosa que la consolidación específica con respecto a los documentos administrativos y a los mensajes en ellos contenidos de la facultad de investigación, una de las que componen el derecho a la información, implícitamente reconocido en el artículo 20 de la Constitución en virtud de la integración normativa del artículo 96 e interpretativa del artículo 10.2» [36]. La referencia a la interpretación según el 10.2 supone acudir

---

[29] Véase al respecto la síntesis que de las diferentes posiciones doctrinales realiza DESANTES GUANTER, J. M.: «Teoría y régimen jurídico de la documentación». *Eudema*. Madrid. 1987. Páginas 118 a 120.

[30] Ponente ROLDÁN MARTÍNEZ. *Aranzadi*, 3369.

[31] Véase la velada crítica de DESANTES GUANTER: «Teoría y ...» Ob. cit. página 159.

[32] No existe en estos momentos una Ley post-constitucional que regule dicho acceso. Se intentó en su momento en desarrollar el 105 b) por medio de la Ley de Protección del Patrimonio Artístico, pero en la discusión parlamentaria se rechazó tal posibilidad.

[33] OLIVA, A. de la: «Límites constitucionales a la obtención y uso de la informática». Boletín del Ilustre Colegio de Abogados de Madrid núm. 6/1984. Página 55. Las referencias que realiza son a:

MUÑOZ MACHADO, S.: «Sobre el acceso de los ciudadanos a los archivos y registros administrativos» presentado en el Seminario sobre «Relaciones Administración-Ciudadano: Información, Documentación y Libertades Públicas», organizado por el Instituto Nacional de Prospectiva en mayo de 1980.

SAINZ MORENO: «El acceso de los ciudadanos a los archivos y registros administrativos (Sentencia del Tribunal Supremo de octubre de 1979)». Revista Española de Derecho Administrativo, núm. 24, 1980. Páginas 180 y ss.

[34] DESANTES GUANTER, J. M.: «Teoría ...». Ob. cit. páginas 49 y siguientes.

[35] DESANTES. Ob. cit. página 155.

[36] DESANTES GUANTER, J. M.: «Teoría ...». Ob. cit. página 162.

Sobre la facultad de investigación y su relación con la facultad de información, véase SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, M.: «La libertad de expresión del militar profesional». U.C.M., Madrid, 1992, págs. 92-96.

Esta «descolocación» del artículo 105 b) ha llevado a DESANTES y a SORIA a afirmar con

a la Declaración Universal de Derechos Humanos, en este caso al artículo 19, y a los tratados internacionales que sobre la materia haya ratificado España.

Los precedentes legislativos más próximos se encuentran recogidos en las legislaciones norteamericana [37] y francesa [38], en donde concurren una normativa de acceso a los archivos administrativos y otra de protección de la intimidad frente al tratamiento automatizado de datos personales.

En nuestra legislación, la apertura más «avanzada» la protagonizaron los artículos 62 y 63.1 de la Ley de Procedimiento Administrativo (17/7/1958) aunque el derecho de información de los expedientes administrativos se limita a los interesados, a conocer el estado de tramitación y a obtener copia certificada de los extremos concretos contenidos en el expediente [39].

---

rotundidad: «Hay una norma en la Constitución a la que no se ha concedido la importancia que tiene para hacer eficaz la facultad de investigación, quizá por su desplazamiento del lugar donde debería haberse incluido, que es el artículo 20. Se trata de la contenida en el artículo 105 b),...» (DESANTES GUANTER, J. M. y SORIA, C.: «Los límites de la información». Ob. cit. Página 80).

[37] La FREEDOM OF INFORMATION ACT (de 4/07/1967, modificada por la Ley 93-502 de 21/11/1974) de los Estados Unidos establece como excepciones:»

(b)(6) personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy» –(ficheros personales y médicos y otros similares cuya revelación constituiría una invasión injustificada de la privacidad personal).

Incluso se establece la posibilidad (*agency may delete identify details*) de borrar detalles de los manuales e intrucciones a funcionarios que se juzgue conveniente evitar una intromisión injustificada en la privacidad personal del individuo –párrafo (a)(2)(C)–. Véase O'BRIEN, D.: «El derecho del público a la información. La Suprema Corte de los E.U.A. y la Primera Enmienda Constitucional» México, 1983. Páginas 211 a 217. Véase DESANTES GUANTER: «Teoría ...». Ob. cit. páginas 145 a 148.

Sobre la protección de la intimidad frente al tratamiento informático de datos personales, véanse:

PRIVACY ACT OF 1974 (United States Doce Annotad-USCA-) con su correspondiente actualización de 1990 en CONGRESO DE LOS DIPUTADOS, Secretaría General: «Protección de datos personales. Documentación preparada para la tramitación del Proyecto de Ley Orgánica de regularización del tratamiento automatizado de los datos de carácter personal». Septiembre, 1991. Páginas 687 y siguientes.

PRIVACY PROTECTION ACT OF 1980. Ibidem. Página 745.

[38] LOI núm. 78-753, de 17/7/1978 modificada por la LOI núm. 79-587, de 11/7/1979 y el Decreto núm. 88-465, de 28/4/1988 PORTANT DIVERSES MESURES D'AMELIORATION DES RELATIONS ENTRE L'ADMINISTRATION ET LE PUBLIC ET DIVERSES DISPOSITIONS D'ORDRE ADMINISTRATIF, SOCIAL ET FISCAL. Véase en CONGRESO DE LOS DIPUTADOS: «Protección de datos personales ...» Ob. cit. páginas 769 y siguientes.

DECRET núm. 88-465, de 28/4/1988, RELATIVA LA PROCEDURE D'ACCESAUX DOCUMETS ADMINISTRATIFS. Véase en CONGRESO DE LOS DIPUTADOS: «Protección de datos personales...» Ob. cit. páginas 773 y siguientes.

Véase tambiún DESANTES GUANTER: «Teoría ...» Ob. cit. páginas 148 a 151.

Respecto al tratamiento automatizado de datos personales: LEY núm. 78-17, de 6/1/1978, SOBRE INFORMATICA, FICHEROS Y LIBERTADES (Traducción DARANAS PELAEZ). Véase en CONGRESO DE LOS DIPUTADOS: «Protección de datos personales ...» Ob. cit. páginas 755 y siguientes.

[39] En concreto el artículo 62 de la LPA establece:

Los interesados en un expediente administrativo tendrán derecho a conocer, en cualquier momento, el estado de tramitación, recabando la oportuna información de las oficinas correspondientes.

Por su parte el artículo 63.1 dice:

El artículo 4.1 de la Ley 12/89, de 9 de mayo, de la Función Estadística Pública al establecer los principios generales en la recogida de datos, entre ellos el de transparencia, incurre en una cierta contradicción:

La recogida de datos con fines estadísticos se ajustará a los principios de **secreto, transparencia,** especialidad y proporcionalidad.

Claro que el artículo 4.3 de dicha Ley se encarga de «descafeinar» el principio de transparencia:

En aplicación del principio de transparencia, los sujetos que suministren datos tienen derecho a obtener plena información, y los servicios estadísticos obligación de proporcionarla, sobre la protección que se dispensa a los datos obtenidos y la finalidad con la que se recaban.

Con lo cual la transparencia que mucho prometía se limita a «la protección que se dispensa a los datos» y a la «finalidad de la toma de datos». Evidentemente esta no es la transparencia a la que nos referimos, ni a la que se refiere el artículo 105 b) de la Constitución.

En este momento en nuestro país existe una gran dispersión normativa en lo que se refiere a la transparencia administrativa y/o al secreto [40].

Los interesados podrán solicitar que se les expida copia certificada de extremos concretos contenidos en el expediente.

El desarrollo de esa función de «información y documentación» (enunciado del capítulo en donde se recogen los mencionados artículos) se realizará por las oficinas de información previstas en el artículo 33.

1. En todo Departamento ministerial, Organismo autónomo o gran unidad administrativa de carácter civil se informará al público acerca de los fines, competencia y funcionamiento de sus distintos órganos y servicios mediante oficinas de información, publicaciones ilustrativas sobre tramitación de expedientes, diagramas de procedimiento, organigramas, indicación sobre localización de dependencias y horarios de trabajo y cualquier otro medio adecuado.

Véanse la Orden de 22 de octubre de 1958 (BOE 3/11/58) por el que se dictan normas sobre el funcionamiento de las oficinas de información, y el Decreto 93/1965, de 28 de enero, por el que se regula el Centro de Información Administrativa y los Servicios de Información Administrativa de los Departamentos ministeriales.

[40] Sirvan de ejemplo, además de las de ámbito general –Ley 9/68 de Secretos Oficiales, amén de la normativa complementaria de la misma– la Orden de 30 de julio de 1982 sobre limitación de acceso a la información contenida en las bases de datos fiscales, o la Ley 14/86 General de Sanidad, de 25 de abril que se refiere en su artículo 10:

Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias:

2. A la información sobre los servicios sanitarios a que puede acceder y sobre los requisitos necesarios para su uso.

3. A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público.

Recordemos que recientemente ha sido modificado el Código Penal por la Ley Orgánica 9/91 de 22/3/1991. El artículo 367 ha quedado redactado así:

El funcionario público o autoridad que revelare los secretos o cualquier información de que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados será castigado con las penas de suspensión y multa de 100.000 a 200.000 pesetas.

Si de la revelación a que se refiere el párrafo anterior resultare grave daño para la causa pública o para tercero, las penas serán las de prisión menor e inhabilitación especial.

Si se tratare de secretos de un particular, las penas serán las de arresto mayor, suspensión y multa de 100.000 a 500.000 pesetas.

La conclusión se ceñiría a resaltar la necesidad de proceder a hacer transparente las actividades de todas las administraciones –central, autonómica y local–. Ello exige no solamente un esfuerzo legislativo sino también formativo que erradique vicios de secretismo del funcionariado.

En definitiva, si buscamos una comunidad en donde sean efectivos los principios de libertad e igualdad se deberán potenciar todos aquellos mecanismos mediante los cuales el ciudadano participe plenamente en los beneficios de una sociedad avanzada.

V. LA TRANSPARENCIA COMO NECESIDAD SOCIAL

En palabras de ALVAREZ-CIENFUEGOS, «son muchos lo que hoy califican la información como el auténtico poder de las sociedades avanzadas. Los Estados, las asociaciones, las empresas son tanto o más poderosas en cuanto que disponen de grandes volúmenes de información. El conocimiento general y científico en particular exigen hoy en día el procesamiento, acceso y la valoración de fuentes de información múltiples y diversas» [41].

Por tanto la puesta a disposición del público de las bases de datos permitiría una difusión del poder, así como una mayor rentabilidad de muy diversos sectores económicos que obtendrá con ello información que les permita cumplir sus objetivos: empresas de comunicación, empresas de marketing directo, establecimientos industriales etc...

Como ejemplo, podemos imaginarnos a un servicio técnico de vehículos de la marca «S» que quiere establecerse en una determinada comarca. Para dicha empresa es fundamental conocer sus potenciales clientes y, llegado el caso, enviarles publicidad sobre sus servicios. En definitiva conocer quiénes son propietarios de vehículos «S», que vivan en un radio de 80 kilómetros del taller, la antigüedad de los vehículos, etc. Esa información se encuentra en la Dirección Provincial de Tráfico. En una administración transparente, esos datos se pondrían a disposición del taller o de las empresas encargadas

---

El artículo 7, aún vigente, de la Ley 14/66 de Prensa e Imprenta de 18/3/1966 establece:

1. El Gobierno, la Administración y las Entidades públicas deberán facilitar información sobre sus actos a todas las publicaciones periódicas y agencias informativas en la forma que legal o reglamentariamente se determine.

2. La actividad de los expresados órganos y de la Administración de Justicia será reservada cuando por precepto de la Ley o por su propia naturaleza sus actuaciones, disposiciones o acuerdos no sean públicos o cuando los documentos o actos en que se formalicen sean declarados reservados.

Dicho artículo 7 fue desarrollado por el Decreto 750/66 de 31 de marzo, concretamente en sus artículos 9 a 11.

El proyecto de Ley del Patrimonio Histórico Español incluía un desafortunado artículo 57 que hacía referencia al artículo 105.b). Afortunadamente dicho precepto quedó limitado al derecho de acceso a la documentación histórica de organismos públicos y privados en los términos del artículo 49.2 de dicha Ley 13/85 de Patrimonio Histórico Español.

[41] ALVAREZ-CIENFUEGOS SUÁREZ, J. M.: «El derecho a la intimidad personal, la libre difusión...». Ob. cit. Página 183.

de planificar la instalación del mismo y su publicidad. Hoy en día esto no es así en nuestro país.

Pero la situación puede ser aún más contradictoria. El Registro Mercantil se rige por disposiciones específicas y su finalidad es dar a conocer al público las empresas constituidas, así como sus órganos rectores entre otros datos. Sin embargo, si un periodista que investiga una red de tráfico de influencias pregunta en el Registro Mercantil en qué empresas es consejero el señor GGG, se encontrará con que esa información no se le facilita. Si la pregunta la realiza el Banco de España o cualquier autoridad del Estado, puntualmente se responderá.

Ante la creciente necesidad de información y el hermetismo de las fuentes, se generan situaciones de irregularidad en donde la corrupción del funcionariado y la existencia de bases de datos privadas son la nota dominante. Tal es el caso de la red de tráfico de datos descubierta a finales de 1991 en Madrid. En definitiva «la sociedad, para su desarrollo, tal y como está concebida hoy día demanda datos y más datos» [42], por lo que «resulta difícil una política que limite o condicione el acceso a la información» [43].

VI. TRANSPARENCIA E INTIMIDAD

Tanto el derecho a la intimidad informática como la transparencia administrativa se contempla la facultad de acceder a los ficheros informatizados. Ahora bien, existen una serie de diferencias entre ambos supuestos. En el caso del derecho a la intimidad informática, el dato es personal, el sujeto legitimado es únicamente el interesado y el sistema informático puede ser tanto privado como público. En el supuesto del artículo 105.b, el dato puede ser personal o de otra índole –por ejemplo, los volúmenes de ventas de cebollas en las campañas 1985/1991–, el sujeto legitimado es cualquier ciudadano y el sistema informático es de la Administración.

Los bienes jurídicos protegidos en uno y otro caso son muy diferentes. La opinión pública libre en el caso de la transparencia administrativa –en tanto en cuanto que entendemos que se constituye en una faceta particular de la facultad de investigar del derecho a la información– y la intimidad de las personas en el supuesto del derecho a la intimidad informática.

La redacción del artículo 105 b) parece apuntar a una colisión entre la transparencia administrativa y la intimidad, hasta el punto de establecer la intimidad como una excepción al principio de transparencia de la Administración. La cuestión es ¿por qué la intimidad opera como una excepción a la transparencia de las bases de datos de la Administración? La respuesta pasa por considerar que la divulgación de determinados datos pueden acarrear

[42] Ibidem.
[43] Ibidem.

consecuencias negativas –robos, extorsiones, secuestros...– para las personas cuyos datos figuran en el fichero automatizado [44] y vulnerar derechos personalísimos como el honor, la intimidad personal o la intimidad informática.

Sin embargo, varias son las reflexiones que podemos hacernos al respecto. Debemos considerar que los males que le pueden suponer a una persona por conocerse determinados datos de su vida privada, deben ser atajados por la actividad policial que impida el delito, no por la prohibición de conocer esos datos, que muchas veces se obtienen de una observación de la realidad cotidiana. Incluso el hecho que los delincuentes obtengan de los ficheros administrativos, datos para cometer un delito pueden servir de indicio a los servicios policiales al rastrear las peticiones de información que se han realizado.

Además las peticiones de información integrarían una base de datos importante desde el momento que serviría como punto de partida para la actuación de la Agencia de Protección de Datos.

Si se argumenta que la transparencia de datos de la Administración atenta contra la intimidad o el honor de las personas se deben realizar varias precisiones.

En primer lugar los datos pueden significar un atentado directo contra la intimidad, se trata de los llamados datos sensibles. La cuestión se reduce en este caso a recapacitar si la Administración debe de tener esos datos en su poder. Defendiéndose como principio genérico que salvo absoluta necesidad para el funcionamiento de la Administración o para el bien de la sociedad, el Estado no debe de poseer datos sensibles de los ciudadanos –se trataría ya de un atentado contra la intimidad–. Cuando se justifique tal extremo, la excepción tendría su correlativa excepción a la hora de proporcionar datos al público. Con lo cual la oposición a entregar datos de los archivos públicos a los particulares argumentada a partir de la intimidad de las personas, precisaría una doble justificación: la razón por la cual la Administración tiene esos datos considerados por ella misma como íntimos y la razón por la que considera que esos datos afectan a la intimidad de las personas.

Si los datos que están en poder de la Administración son de los llamados no sensibles, la cuestión vuelve a reproducirse con algunas matizaciones. En primer lugar también sería necesario cuestionarse las razones por las que la Administración tiene esos datos en su poder, o incluso la forma como tiene la Administración los datos. Evidentemente para realizar un censo de vivien-

[44] Posiblemente el caso más conocido fue el del Sr. Suñer, industrial valenciano que figuraba en los primeros puestos de la lista de mayores contribuyentes a Hacienda publicados en los primeros años de la democracia. Dicho empresario fue secuestrado con el objeto de pedir un rescate. Desde entonces no se han vuelto a publicar las listas de mayores contribuyentes a la Hacienda Pública, incluso la Orden de 30 de julio de 1982, firmada por el Ministro de Hacienda, García Añoveros, estableció las limitaciones de acceso a la información contenidas en las bases de datos fiscales.

das o de población al Estado para nada le interesa que la señora María Jiménez Pérez ha tenido 15 hijos y 3 abortos, lo que le interesa es el dato agregado que hay 390 mujeres que han tenido ese número de hijos. Se trataría en definitiva del problema de la pertinencia de los datos. Las diferencia con el supuesto anterior vendría del hecho que la intromisión en el derecho a la intimidad informática se produciría por el cruce informático de datos realizado por un particular. En este caso son los mecanismos de protección del derecho a la intimidad informática establecidos en la LORTAD, los encargados de evitar tales situaciones.

En definitiva, la transparencia de las bases de datos obligaría a las administraciones a tener en sus ficheros sólo aquellos registros que fueran precisos para su actuación, pues al estar estos datos a la vista [45] del público cualquiera podría detectar intromisiones en los derechos de la personalidad.

BIBLIOGRAFIA

ALVAREZ-CIENFUEGOS SUÁREZ, J. M.: «El derecho a la intimidad personal, la libre difusión de la información y el control del Estado sobre los bancos de datos» en Davara, M.A. y otros «Encuentros sobre Informática y Derecho 1990-1991». *Universidad Pontificia de Comillas – Aranzadi* 1992.

AMAT LLARI, Eulalia: «El derecho a la propia imagen y su valor publicitario». *Edt. La Ley*. Madrid, 1992.

ARAMENDI, CABELLERO, DOMAICA, MÉNDEZ, PENADÉS y VALLÉS: «Leyes de protección de datos», en II Encuentro sobre la informática en las Facultades de Derecho (Mayo 1988). *Universidad Pontificia de Comillas*. Madrid.

AUDIJE PACHECO, CAMPUZANO ROBLEDO, FERNÁNDEZ MUGUELES Y RUBIO SIERRA: «Consideraciones acerca de una futura Ley española para limitar el uso de la informática», en III Encuentro sobre la informática en las Facultades de Derecho (Mayo 1989). Madrid, 1990.

BELLO PAREDES, Santiago A.: «El Número de Identificación Fiscal, algunas consecuencias de su incardinación en nuestro ordenamiento jurídico» en Davara, M. A. «Encuentro sobre Informática y Derecho 1990-1991». *Universidad Pontificia de Comillas – Aranzadi* 1992.

CONGRESO DE LOS DIPUTADOS, Secretaría General: «Protección de datos personales. Documentación preparada para la tramitación del Proyecto de Ley Orgánica de regularización del tratamiento automatizado de los datos de carácter personal». Septiembre, 1991.

CORTES ESPAÑOLAS: «Constitución española. Trabajos parlamentarios». Madrid, 1980.

[45] Existiría toda otra cuestión que no es el momento de desarrollar aquí, referida a la legibilidad de los datos y más concretamente al empleo de datos codificados.

DESANTES GUANTER, J.M.: «Teoría y régimen jurídico de la documentación». *Eudema.* Madrid, 1987.

DESANTES GUANTER, J.M. y SORIA, C.: «Los límites de la información». *Asociación de la Prensa de Madrid,* 1991. Página 107.

FARIAS GARCÍA, P.: «Libertades Públicas e Información». *EUDEMA*, Madrid, 1988.

FROSINI: «Il diritto alla riservatezza come diritto di libert». *Milano*, 1985.

GIL, L.: «La censura en el mundo antiguo» *Alianza Universidad.* Madrid, 1985.

HERRERO-TEJEDOR, F.: «Honor, intimidad y propia imagen». Madrid, 1990.

LUCAS MURILLO, P.: «El derecho a la autodeterminación informativa». Madrid, 1990

MINISTERIO PARA LAS ADMINISTRACIONES PÚBLICAS, Dirección General de Organización, Puestos de Trabajo e Informática: «Leyes de protección de datos». Madrid, 1988

MUÑOZ MACHADO, S.:«Sobre el acceso de los ciudadanos a los archivos y registros administrativos» presentado en el Seminario sobre «Relaciones Administración-Ciudadano: Información, Documentación y Libertades Públicas», organizado por el Instituto Nacional de Prospectiva en mayo de 1980.

O'BRIEN, D.: «El derecho del público a la información. La Suprema Corte de los E.U.A. y la Primera Enmienda Constitucional» México, 1983.

OLIVA, A. de la: «Límites constitucionales a la obtención y uso de la información». Boletín del Ilustre Colegio de Abogados de Madrid nº 6/1984.

ORWELL, G.: «1984»

PÉREZ LUÑO, A.: «Derechos humanos, Estado de Derecho y Constitución». Madrid, 1984.

«Concepto y concepción de los derechos humanos». Doxa, nº 4. 1987.

«Del Habeas Corpus al Habeas Data» en Davara, M.A. y otros «Encuentros sobre Informática y Derecho 1990-1991». *Universidad Pontificia de Comillas – Aranzadi* 1992.

SAINZ MORENO: «El acceso de los ciudadanos a los archivos y registros administrativos (Sentencia del Tribunal Supremo de octubre de 1979)». *Revista Española de Derecho Administrativo n.º 24*, 1980.

SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, M.: «La libertad de expresión del militar profesional». *UCM*, Madrid, 1992.

SÁNCHEZ, E.: «El Marketing Directo y la Protección de Datos» en revista NOVATICA volumen XVIII nº 96. Marzo-abril, 1992.

Los derechos humanos de la tercera generación. Libertad informática

ENRIQUE SÁNCHEZ JIMÉNEZ
Licenciado en Derecho
(ESPAÑA)

A lo largo de la presente comunicación pretendo hacerles ver cómo la libertad informática se ha ido configurando como un derecho humano de la tercera generación. Para este fin que hoy me propongo voy a comenzar haciendo una breve síntesis sobre qué son los derechos de la tercera generación, para centrarme posteriormente en analizar la libertad informática como tal, y ver cuál es su repercusión en la sociedad actual, dándoles por último, una breve conclusión acerca de este tema.

La humanidad contemporánea parece haber adquirido plena conciencia de la historicidad, la cual halla un motivo de evidencia en diversos textos, todos ellos referentes a los Derechos Humanos, la Constitución Española, la Declaración Universal de los Derechos Humanos y la Declaración de los Derechos del Hombre y del Ciudadano establecida por la Asamblea Constituyente que surge de la Revolución Francesa. Examinados los derechos y libertades que en estos textos se proclaman, observamos coincidencias y discrepancias. El contenido de cada uno de ellos se encuentra limitado por el contexto histórico en que fueron realizados, y así derechos recogidos en nuestra vigente Constitución no se hallan presentes en otros textos. Esto nos hace llegar a la conclusión de que nos encontramos ante Derechos Humanos que no constituyen categorías cerradas y definitivas, sino más bien, *catálogos abiertos y permeables a la incorporación de valores y derechos actuales*, todo ello nacido como respuesta a las exigencias que un ser humano puede encontrar en una determinada época.

La mutación que se produce a lo largo del devenir histórico de los Derechos Humanos, determina la sucesiva aparición de una serie de «generaciones» de derechos. Los primeros Derechos Humanos nacen con la modernidad en el seno de la atmósfera iluminista que inspiró las revoluciones burguesas del siglo XVIII, lo que hace que estos nazcan con una marcada tendencia individualista, como libertades individuales que reconocen poderes al individuo como ser aislado, configurándose así, la primera generación de Derechos Humanos. (PECES-BARBA, G. 1982).

Dicha tendencia sufrió una importante erosión, debido a las luchas sociales llevadas a cabo en el siglo XIX, poniéndose de relieve la necesidad de completar los Derechos Humanos de la primera generación con otros de carácter económico, social y cultural. Esta segunda generación de derechos quedó a su vez consagrada con el tránsito que se produce del Estado Liberal al Estado Social de Derecho.

La distinción entre una y otra, se hace más patente cuando se considera que mientras en la primera los Derechos Humanos son defensivos de las libertades del individuo, exigiéndose la autolimitación y no injerencia del poder público y tutelándose por su mera actitud pasiva y de vigilancia; en la segunda son derechos de participación, requiriéndose una política activa de los poderes públicos y removiéndose los obstáculos que impiden que la libertad e igualdad de los ciudadanos sean reales. No basta con la mera vigilancia de las técnicas jurídicas, sino que se requiere un sistema de prestaciones y servicios públicos. (PÉREZ LUÑO A. E. 1988).

A partir de los años 80, se habla de nuevas reivindicaciones de los Derechos Humanos, que giran en torno a temas como, calidad de vida, la paz o la libertad informática. Esta tercera generación de derechos se presenta como respuesta en términos de libertad y facultad de las personas a la «contaminación de libertades» que se ha producido con la aplicación de nuevas tecnologías.

La tarea de precisar los derechos de la tercera generación es, un «work in progress» ni fácil, ni cómodo y por ello urgente y necesario. (PÉREZ LUÑO A.E. 1991). Para agilizar dicha labor, se pueden dar una serie de rasgos innovadores que van a caracterizar los derechos de la tercera generación:

a) *Una nueva fundamentación;* pues si la libertad y la igualdad fueron los valores guía de la primera y segunda generación, respectivamente, los derechos de la tercera generación tiene como principal valor la solidaridad. Sólo mediante un espíritu solidario de sinergia, es decir, de cooperación y sacrificio voluntario y altruista de los intereses egoístas será posible satisfacer plenamente las necesidades y aspiraciones globales relativas a la paz, la calidad de vida o a la libertad informática. (MASUDA Y. 1984).

b) *Nuevos instrumentos de tutela;* debido a las inmediatas consecuencias que ha tenido en este tema la dimensión generacional de los derechos

fundamentales. Así, se hace necesario completar, la teoría de los status que en su día formuló Georg Jellinek, con otros como el status positivus socialis de Hberle que se encarga de los derechos sociales, (PÉREZ LUÑO A. E. 1986), el status activus processualis de Denninger que pretende dinamizar el procedimiento, (PÉREZ LUÑO A. E. 1991), o el status de habeas data, que en el terreno de la informática, intenta jugar un papel paralelo al del habeas corpus en la tradición de las libertades, reconociéndose al ciudadano la posibilidad de examinar y corregir cuantos datos suyos procese un banco de datos. (PÉREZ LUÑO A. E. 1987).

c) *Nuevas formas de titularidad;* debido a las nuevas situaciones y posiciones jurídicas subjetivas que surgen en la actualidad. Es preciso reconocer a la generalidad de los ciudadanos la legitimación para defenderse de las agresiones a bienes colectivos o intereses difusos que por su naturaleza no pueden tutelarse bajo la vieja óptica de la lesión individualizada. De ahí que sea defendida la acción popular como medio idóneo para la superación de la concepción individualista del proceso. Todo esto, exige correlativamente una ampliación de la legitimación pasiva, para superar ciertas trabas formales que impedían actuar contra los daños colectivos que quedaban en la impunidad. (PÉREZ LUÑO A. E. 1989a).

De este modo, la Filosofía del Derecho, no puede permanecer impasible ante las nuevas transformaciones experimentadas en el seno de la sociedad moderna. Uno de estos cambios, viene directamente determinado por la recepción de las nuevas tecnologías en nuestro hacer cotidiano [1].

La aparición de los ordenadores abrió nuevas perspectivas tanto en el terreno jurídico como en el del pensamiento. En el jurídico aparecen nuevos delitos, nuevos derechos que proteger... En el del pensamiento porque resulta imprescindible reflexionar sobre la influencia que estos objetos van a ejercer sobre los hombres, sus formas de vida, sus trabajos... Toda innovación tecnológica ha producido en muy breve plazo, un cambio en la forma de pensar de aquella parte de la humanidad afectada. La tecnología del ordenador no va a ser una excepción a esta regla, por lo que, resulta necesario también su estudio desde la óptica de la Filosofía del Derecho. (GONZÁLEZ-TABLAS R. 1986).

Haciendo un breve recorrido por las numerosas disposiciones surgidas a principios de los años 70, cuyo objeto es la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, hay que significar que éstos se agrupan en conjuntos, cada uno con objetivos diferentes.

Un primer conjunto de normas surge como instrumento de garantía encaminados a establecer determinados límites a la utilización de la informática.

---

[1] TRUYOL SERRA A. (1982: 118 afirma: «la Filosofía del Derecho no puede dejar de enfrentarse con lo que, con una palabra sin duda algo gastada, pero finalmente difícil de sustituir, podemos denominar el reto de la sociedad de la información».

Al pretenderse reglamentar el funcionamiento de los bancos de datos se consideró como sistema más eficaz de protección una ley general basada en la autorización previa de los bancos de datos y un control posterior.

Un segundo bloque de normas pretende asegurar, la calidad de las informaciones mediante la introducción de cláusulas que protejan los datos especialmente sensibles, lo que contribuye a conformar el derecho a la libertad informática, al reconocer y tutelar los derechos al acceso y control de las informaciones por parte de las personas concernidas.

Una tercera generación de normas aparece hoy como respuesta a nuevos problemas, como es la sustitución de los grandes ordenadores con los que operaban los bancos de datos por los ordenadores personales, los cuales acarrean una numerosa difusión de los bancos de datos.

El derecho a la autodeterminación informativa, desde que hizo su aparición en la R.F.A., ha suscitado un vivo debate acerca de su consideración como un derecho fundamental, o más bien, como una especificación del derecho general a la personalidad.

Esta última postura fue defendida por quienes creían que la autodeterminación informativa o libertad informática era un aspecto de la vida privada y ésta a su vez, una derivación del derecho a la dignidad del hombre y más concretamente del derecho al libre desarrollo de la personalidad ya que la Constitución alemana no reconoce un derecho fundamental a la intimidad, siendo todo ello aceptado por la labor interpretativa llevada a cabo por la Jurisprudencia del Tribunal Constitucional Federal. (PÉREZ LUÑO A. E. 1989b).

Adalbert Podlech mantiene una peculiar postura acerca de este tema y es que el derecho al libre desarrollo de la personalidad se divide en una libertad de acción entendida como libertad para hacer u omitir determinados actos y una autodeterminación informativa, es decir, libertad para determinar en qué casos pueden ser revelados datos que le conciernen, condicionándose y complementándose ambas libertades entre sí.

Otras veces las resistencias a reconocer como derecho fundamental la autodeterminación informativa se centra, como así lo cree Spiros Simitis, en el temor a que su admisión conlleve a consagrar una especie de derecho a la propiedad privada sobre los datos personales, corriendo el riesgo de considerarlos derechos patrimoniales y por tanto limitando su interpretación a estos conceptos.

En opinión del profesor PÉREZ LUÑO es correcto el evitar que la autodeterminación informativa sea considerada desde un punto de vista individual y patrimonial ya que ello comprometería su evidente dimensión social y comunitaria, pero discrepa acerca de que el logro de este objetivo, implique la negativa a considerar la autodeterminación informativa como un derecho fundamental. (PÉREZ LUÑO A. E. 1989c).

Dicha opinión se halla sustentada en base a unos criterios que a continuación voy a exponer:

Un primer criterio reside en la *dimensión social de la libertad informática.* Las reservas a considerar la libertad informática como un derecho fundamental partían de su vinculación con el derecho a la intimidad, el cual, en principio fue concebido como una libertad de signo individual, dejando por completo a un lado el que este derecho deja de ser entendido como un derecho a la soledad y aislamiento para ser concebido en nuestros días, como un derecho al poder de control sobre las informaciones particulares de cada sujeto. (WARREN Y BRANDEIS, 1990).

En palabras de ADALBERT PODLECH la intimidad más que un estado de autoconfinamiento, supone una determinada calidad de la relación con los otros. Resulta, por tanto, insuficiente concebir la intimidad como un derecho de garantía (status negativo) frente a cualquier tipo de intromisión en la esfera privada de una persona, sin contemplarla como un derecho activo de control (status positivo) sobre las informaciones que atienen a un particular. (PÉREZ LUÑO A. E. 1986b).

Un segundo criterio descansa en que *el negar la autonomía del derecho, para englobarlo en el derecho al libre desarrollo de la personalidad, haría muy difícil su relación con otros derechos fundamentales.*

Al igual que ocurre en el sistema constitucional alemán, en el español la autodeterminación informativa o libertad informática a partir de su reconocimiento inmediato en los art. 18.4 y 105.b se ha relacionado con otros preceptos constitucionales. De esta forma, la libertad informática, se remite al artículo 1.1 que define nuestra política como «Estado social y democrático de derecho que propugna valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político» exigiéndose esto, hacerse patente a través de un equilibrio de poderes de acceso y control a las informaciones, lo que encuentra confirmación en el compromiso constitucional de hacer reales y efectivas la libertad e igualdad de los ciudadanos que propugna el art. 9.2. No hay que olvidar el nexo de unión con el derecho a la dignidad y al libre desarrollo de la personalidad proclamados en el art. 10.1, ni con el derecho a la intimidad del art. 18, así como con otras libertades como la ideológica (16.1), de expresión (20.1,a) etc...

Estas concordancias sólo se dan en la medida en que se concibe la libertad informática como un derecho fundamental autónomo. Si se concibe el habeas data y las demás facultades que conforman la libertad informática como un mero apéndice de otros valores su enlace debería hacerse por vía indirecta, es decir, a través de esos valores en los que se reputa incluida.

Un tercer criterio relevante es el propio carácter dinámico de los derechos fundamentales, ya mencionado. En muchas ocasiones al no reconoci-

miento del derecho fundamental subyace la concepción de catálogo cerrado y completo de estos, pero esto no debe ser así.

Una sociedad libre y democrática debe estar siempre abierta y ser sensible a la aparición de nuevas formas de agresión a la libertad y de nuevas necesidades que fundamenten derechos nuevos. Así ocurre respecto a la libertad informática que surge como respuesta a las amenazas que dimanan del empleo de nuevas tecnologías, en especial de la informática y de la telemática, las cuales pueden invadir la intimidad y condicionar la capacidad de los ciudadanos para actuar libremente.

+ Un último criterio reside en el *reforzamiento de su garantía.*

Para garantizar la protección de la libertad informática conviene concebirla como un derecho fundamental autónomo, dotado de medios específicos de tutela. Por contra, disuelta en el ámbito de otros valores o derechos, la autodeterminación informativa corre el peligro de relativizarse y ver comprometida su efectiva realización.

Como conclusión hay que destacar que el alcance de la libertad informática, es un reto abierto y constante en la teoría y práctica actual sobre los derechos y libertades, y así, no es reconocida en determinados países y sí en otros, como es el caso en la actualidad de Brasil que ha reconocido la libertad informática como derecho fundamental en una reciente reforma de su texto constitucional.

Como espero que a lo largo de la presente comunicación haya quedado aclarado, la libertad informática cumple las dos funciones normales que han de seguir los derechos fundamentales: asegurar la identidad de las personas ante el riesgo de que sea invadida por determinados usos de las nuevas tecnologías, poniendo en sus manos los mecanismos procesales pertinentes para acceder y controlar las informaciones que la conciernen **(habeas data)**, y contribuir a conformar un orden político basado en la participación en los procesos de información que definen al ejercicio de poder en las sociedades informatizadas actuales.

BIBLIOGRAFIA

GONZÁLEZ-TABLAS SASTRE, R.: «Filosofía del derecho e informática», Sevilla, Tesis Doctoral, 1986, p.1.

MASUDA, Y.: «La sociedad informatizada como sociedad postindustrial», (traducción al castellano J. OLLERO y F. ORTIZ), Madrid, *Tecnos y Fundesco*, 1984, pp. 120 ss.

PECES -BARBA, G.: «Tránsito a la modernidad y derechos fundamentales», Madrid, Mezquita, 1982.

PÉREZ LUÑO, A. E.: «Derechos Humanos, Estado de Derecho y Constitución», Madrid, *Tecnos, SA* 1986, pp. 87 ss.-a pp. 324 ss-b.

«Nuevas tecnologías, sociedad y derecho», Madrid, *Fundesco*, 1987, pp. 85 ss.

«Concepto y concepción de los derechos humanos, (acotaciones a la ponencia de Francisco Laporta)», en D, vol. 4, 1988, pp. 55 ss.

«Libertad informática y leyes de protección de datos personales», Madrid, Centro de Estudios Constitucionales, 1989, pp. 142-143-a, pp. 155-156-b, pp. 156 ss.–c.

«Las generaciones de derechos fundamentales», Revista del Centro de Estudios Constitucionales, n.º 10, 1991, pp. 210 ss.

WARREN, S. D. Y BRANDEIS, L.D., The Right to Privacy, HLR, 1990, n.º 4, pp. 193 ss.

COLOQUIOS

INTERVENCION DE D. GUILLERMO OROZCO. COORDINADOR: Queremos agradecer desde la Mesa la intervención a los participantes, así como la calidad y claridad de sus exposiciones y la profundidad de los temas. Ahora vamos a abrir un breve coloquio.

PREGUNTA. La pregunta es para D. ALFONAO DE JULIOS CAMPUZANO. Al cambiar el tema a su comunicación «Seguridad del Tráfico mercantil» por «El Derecho a la intimidad» ¿es porque estima que el de la intimidad es aún más amplio que el del tráfico mercantil?

RESPUESTA DE D. ALFONSO DE JULIOS CAMPUZANO: El cambio del título respondió a que yo pretendía abordar el Tráfico Mercantil, lo que ocurrió es que después, al trabajar sobre el tema, surgió en mí una inquietud, creo que más amplia, entonces quise englobarla en el título y en el propio desarrollo de la comunicación. La inquietud que preside la comunicación, es que el Proyecto de la LORTAD, no resuelve definitivamente, el ámbito de la intimidad en el estado social y la propia dinámica del Estado y el ámbito de la intimidad restringido, quizás en exceso referido a conceptos o a ámbitos, ya sea lo estrictamente físico o ideológico que dejan al individuo, quizás, en una situación un poco de desamparo en muchos aspectos. Para todo esto, quizás sea lo conveniente remitirse a la sesión de esta tarde, en la que se va a abordar la LORTAD más en profundidad, pero lo cierto es que la protección que la LORTAD, quizá el tema patrimonial no lo contempla, bueno, lo contempla, pero parece que las garantías que ofrece no son de suficiente peso. Esta duda, o este temor lo comparto con otra serie de personas y, en especial, con el Profesor PÉREZ LUÑO, de quien tuve la ocasión de exponer una ponencia suya en el Congreso de Informática y Derecho, dirijido por el Profesor DAVARA, en Madrid, y sobre este tema albergo la esperanza de que en el futuro, si no es en el trámite parlamentario, quizás la propia aplicación jurisprudencial, la labor cumplimentada que la jurisprudencia, venga a esclarecer este tipo de duda o éste abanico de dudas que albergamos en esta materia.

PREGUNTA: Quería preguntar al Profesor MONTERO acerca de su intervención, tres cosas: Si efectivamente en Bélgica y en Francia la obligación de los productores de información, las empresas que venden información de carácter mercantil o financiero sobre otras terceras, si efectivamente esa

obligación de informar a los sujetos sobre los que tienen información en sus bancos de datos se cumple. La segunda pregunta es, ¿cual es la vía procesal, cual es el procedimiento que se utiliza en estas legislaciones belga y francesa para hacer este tipo de reclamaciones cuando la información vendida por el productor de estos datos es incompleta, falsa o poco veraz?, y en tercer lugar, ¿si conoce usted de la jurisprudencia de los países de que hablamos, el monto o la significación de las indemnizaciones cuando ha existido alguna sentencia condenatoria para estas empresas, si es una indemnización significativa? Gracias

RESPUESTA DE D. ETIENNE MONTERO: Creo que quizás hubo una confusión. He expuesto las obligaciones puestas a cargo de las agencias de información comercial tradicionales, es decir, que existen antes del desarrollo de los servicios electrónicos de información. En este contexto no existe la obligación de informar a la empresa registrada, no existe, es un nuevo concepto que aparece con las legislaciones "Privacy"; antiguamente las agencias de información comercial no tenían la obligación de informar a la persona registrada de la existencia del tratamiento. Para responder a la segunda pregunta, el tipo de acción es una acción de responsabilidad civil, sencillamente. He expuesto el Derecho de la responsabilidad civil y es una acción de responsabilidad civil, porque no existían todavía los derechos y las acciones previstas en las legislaciones «privacy», que todavía, por ejemplo, no existe en Bélgica. Hay un proyecto de Ley, como en España, para protección de la vida privada, pero todavía esta Ley en Bélgica no existe, en Francia sí. Lo de la indemnización, muchas veces es poca cosa, es el daño moral. Se indemniza el daño moral y nada más, pero a veces se puede indemnizar mucho más cuando una persona pide una información a una agencia de información comercial y es una información falsa y por eso contrata con otra empresa y si sigue un daño financiero comercial importante puede ser indemnizado totalmente.

SESION II

MESA N.º 2.–PROTECCION DE DATOS II
(Análisis de la LORTAD)

La cancelación de datos personales en ficheros de titularidad pública en el proyecto de LORTAD

LUIS MIGUEL ARROYO YANES
Licenciado en Derecho
Profesor asociado de la Universidad de Cádiz en la materia de Derecho Administrativo en el Dpto. de Derecho Público
(ESPAÑA)

I. INTRODUCCION

Uno de los elementos esenciales de las legislaciones de protección de datos es la concreción que éstas hacen del llamado derecho a la *libertad informática* o a la autodeterminación informativa, y que se manifiesta, entre otros, a través de los derechos específicos de acceso y conocimiento de los bancos de datos, así como en el de rectificación y cancelación de los datos inexactos o indebidamente procesados[1].

Como no podía ser de otro modo el Proyecto de Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Caracter Personal (en adelante lo citaremos como Proyecto, o, como LORTAD) ha sido receptivo a ofrecernos una determinada formulación de los indicados derechos, sin los

[1] Vid. A. E. PÉREZ LUÑO: «Derechos humanos, Estado de Derecho y Constitución», Madrid, *Tecnos*, 1984, p. 370 y ss. Id. Introducción a los sistemas informatizados de documentación jurídica, en A. E. PÉREZ LUÑO (dir.) «Problemas actuales de la documentación y la informática jurídica». Madrid, *Tecnos*, 1987, pp. 27-48, esp. p. 45. Para una elaboración doctrinal de la noción de autodeterminación informativa, vid. E. DENNINGER. El derecho a la autodeterminación informativa, en A. E. PÉREZ LUÑO (dir.). «Problemas actuales...» Ob. cit., pp. 268-276

cuales mal hubieramos podido considerar al mismo como susceptible de garantizar una mínima protección a la indicada libertad informatica[2].

Entre los referidos derechos ocupa un lugar destacado el llamado de cancelación de datos, mediante el cual se manifiesta, mejor que en ningún otro supuesto entre los que cabe desglosar dichos derechos, el posible control que el ciudadano puede llegar a tener sobre la información que obra sobre él en una concreta base de datos. Se trata, por consiguiente, de un derecho que permite conocer a través del examen del alcance y contenido que pueda haberle otorgado una determinada ley de protección de datos, cuales puedan ser las bases sustentadoras y la concepción, amplia, media o restrictiva, que respecto a la intervención de los ciudadanos interesados estén barajando sus redactores.

Nosotros nos proponemos en esta comunicación apuntar únicamente cuál pueda ser el significado, contenido y límites del indicado derecho de cancelación en lo que se refiere a los ficheros de titularidad pública, ésto es, en el caso de aquellos ficheros que han sido creados y son gestionados por las Administraciones y entidades públicas para el eficaz cumplimiento de sus fines[3]. En este sentido aprovecharemos esta operación para proceder a un seguimiento de las principales previsiones de la LORTAD en materia de derechos de los ciudadanos sobre los bancos de datos.

II. EL TERMINO CANCELACION

Antes de proceder a situar sistemáticamente el de cancelación dentro del conjunto de derechos que se recogen en el Proyecto, se hace necesario un breve apunte sobre el significado de este término.

Prácticamente todas las leyes de protección de datos hacen referencia a una operación jurídica tendente a eliminar, a borrar de las memorias informáticas los datos existentes en ellas, a instancias de los ciudadanos interesados. En este sentido resulta suficientemente expresivo el empleo de los términos *erase* o *effacer* imperantes, respectivamente, en los sistemas jurídicos anglo-

---

(2) Como subraya la propia Exposición de Motivos (apartado III): «en concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la ley». El Proyecto dedica un título específico, el tercero, a los llamados derechos de las personas, en cuyos arts. 12 a 17 se dedica a normar su problemática.

(3) No puede dejar de destacarse el papel cada vez más relevante que ocupan las organizaciones públicas en el manejo de datos personales de los ciudadanos, en muchos casos conteniendo sus bancos de datos información especialmente sensible sobre los mismos. Para un examen de esta cuestión pueden consultarse, entre otros, los artículos de J. L. VILLAR PALASÍ. Informática, Derecho y Cambio Social, en AA.VV. Jornadas sobre Informática y Derecho. Madrid, 1985, (sin paginación). J. M. CASTELLS ARTECHE. Aproximación a la problemática de la Informática y Administración Pública, en AA.VV. Jornadas Internacionales sobre Informática y Administración Pública. Oñati, Instituto Vasco de Administración Pública, 1986, p. 25-53. V. FROSINI. Informática y Administración Pública, en Revista de Administración Pública, 105, septiembre-diciembre 1984, pp. 447-458.

sajones y francófonos, para referirse a dicha realidad jurídica en términos incontestables.

En nuestro ordenamiento el término cancelación posee un significado equívoco, debido principalmente a que es empleado para definir una variabilidad de supuestos de contenidos jurídicos diferentes, y que no guardan demasiada conexión entre sí, desconociéndose en nuestro Derecho positivo tal figura como instituto autónomo: existen distintas hipótesis de cancelación pero la doctrina no ha procedido aún a examinarla a nivel dogmático de forma unitaria[4].

Así, se emplea frecuentemente en el Derecho Registral y en el Derecho penal español para hacer referencia a determinadas anotaciones susceptibles de incorporarse a los Registros de la Propiedad y al Central de Penados y Rebeldes, anotaciones que a pesar de ser definitivas, en líneas generales, no comportan la eliminación física de las que han sido objeto de cancelación, sino sólo su pérdida de vigencia o su extinción parcial o total[5].

Llegado a este punto cabe plantearse la pregunta, crucial para nuestros intereses, de cual es, o puede ser, la noción que maneja el Proyecto del término cancelación, y si éste guarda relación o no con ese significado que

---

[4] En este sentido son trasladables aquí las consideraciones que se realizan desde la doctrina italiana al término cancellazione, equivalente a nuestra cancelación. Vid. S. SATTA. Voz Cancellazione, en AA.VV. Enciclopedia del Diritto. Milano, Giuffr, 1959, vol. V, pp. 1064-1066, esp. p. 1064. Un eco de esta problemática en nuestra doctrina, aunque no excesivamente completo, en L. RIERA AISA. Voz Cancelación, en AA.VV. Nueva Enciclopedia Jurídica. Barcelona, F. Seix Editor, 1978, tomo III, pp. 618-625, esp. p. 618.

Prueba de que la utilización del equívoco término cancelación no es exclusiva de los autores del proyecto de LORTAD lo constituye el proyecto de ley de protección redactado para Italia por LOSANO que describe la cancelación, en su definición de términos informáticos, como «hacer inaccesibles los datos personales» que se someten a semejante operación. A nuestro juicio, y como explicaremos seguidamente, dicha definición no puede aceptarse en esos extremos debido a que no resuelve la cuestión principal que plantea la cancelación: si los datos van o no a permanecer en la memoria informática (hacerlos inaccesibles supondrá que los mismos siguen estando recogidos en dicha memoria, algo muy distinto a su eliminación o borrado). Vid. M.G. LOSANO. Un progetto di legge sulla protezione dei dati personali. Il Diritto dell' Informazione e dell' Informatica, 2, maggio-agosto 1987, pp. 465-485, el proyecto aparece recogido en p. 474 y ss.; hay traducción española de este trabajo debida a M. ATIENZA. Un proyecto de ley sobre la protección de los datos personales en Italia, en AA. VV. Libertad informática y leyes de protección de datos personales. Madrid, Centro de Estudios Constitucionales, pp. 63-94, el proyecto aparece recogido en p. 75 y ss.

[5] Para la problemática que esta cuestión plantea en Derecho Registral puede verse el brevísimo pero esclarecedor trabajo de J. M. CHICO ORTIZ. Voz Cancelación, en AA.VV. Diccionario Jurídico Espasa. Madrid, Fundación TOMÁS MORO-ESPASA CALPE, 1991, pp. 133-134. Por lo que se refiere a la problemática en materia de antecedentes penales – que, dicho sea de paso, si están informatizados en ficheros quedan fuera del ámbito del Proyecto, no así los policiales– resulta operativo el artículo 118 del Código Penal, operando en esta materia el Real Decreto 2112/83, de 28 de junio (B.O. de 30 de junio), cuyo artículo 2 únicamente prevee «la eliminación definitiva de las correspondientes anotaciones a todos los efectos» en los supuestos del artículo 1.b) (determinadas faltas que dejan de tener acceso al Registro) y 2 del indicado Decreto (transcurso de plazos de los artículos 113 y 115 del Código Penal).

viene dándosele a nivel registral.[6] Para comprender el sentido exacto del término hemos de adentrarnos en los antecedentes del actual Proyecto, subrayando de paso el hecho de que los anteproyectos y proyectos anteriores al que nos ocupa han venido utilizando con frecuencia la palabra cancelación para referirse al mismo hecho jurídico que nos ocupa.[7] En este orden de cosas cabe recordar cómo el denominado *Anteproyecto de Ley Orgánica de Regulación del Uso de la Informática para la Protección de los Datos Personales*, tras detallar en su artículo 35 en qué supuestos procedería la cancelación, establecía en el 36 lo siguiente:

«La cancelación de los datos no implicará necesariamente la destrucción física de los mismos, pudiendo conservarse en el fichero siempre que constare la circunstancia de la cancelación y la obligatoriedad de que toda comunicación sobre dichos datos hiciere constar su condición de cancelados[8].»

Tomando como base este precepto la doctrina manifestó ya entonces sus dudas sobre la homologación del término cancelación con su equivalente francés (effacement des données), destacando la idea de que cancelar suponía en terminología informática únicamente añadir un carácter de cancelación a un dato o a una información expresa de que no podía ser utilizada.[9] En

---

[6] Nuestro Diccionario de la Real Academia ofrece dos acepciones del vocablo cancelación, la técnica empleada en el Registro de la Propiedad, y la acción y efecto de cancelar. El vocablo cancelar posee también dos acepciones: anular, hacer ineficaz un instrumento público, una inscripción en registro, una nota o una obligación que tenía autoridad o fuerza; y, en sentido figurado, borrar de la memoria, abolir, derogar. Vid. Diccionario de la Real Academia de la Lengua. Madrid, Real Academia, 1984, vigésima edición.

[7] Vid., en este sentido, los arts. 14 y ss. de la proposición de ley de Protección de los Derechos y Libertades en relación con el uso de la informática y las telecomunicaciones presentada por el Grupo Parlamentario Mixto-Agrupación I.U.–E-C– durante la III Legislatura, B.O.C.G.– Congreso de los Diputados, serie B, 23 de junio de 1988, num. 120-1, y durante la IV Legislatura, con el mismo título, y por lo que se refiere a la cancelación con el mismo articulado, por el Grupo Parlamentario de I.U.–I.C. B.O.C.G.–Congreso de los Diputados, serie B, 22 de diciembre de 1989, num. 17-1. Pueden consultarse los mismos en GONGRESO DE LOS DIPUTADOS. Protección de Datos. Documentación preparada para la tramitación del proyecto de LORTAD. Documentación num. 87, Madrid, septiembre 1991, vol. I, p. 143 y ss. 233 y ss.

[8] El indicado artículo pasaría a ser el 34, sin variación alguna, en la última versión del indicado anteproyecto de fecha 10 de diciembre de 1985. Puede consultarse el mismo en AA.VV. Problemas legislativos de la protección de datos. Conferencia Internacional celebrada en Madrid los días 11, 12 y 13 de junio de 1984. Actas y Documentos. Madrid, Servicio Central de Publicaciones de la Secretaría de Estado para la Administración Pública, 1986, p. 121 y ss.

El artículo 35 establecía lo siguiente. 1. Si del ejercicio del derecho de acceso resultara que los datos de carácter personal referente al interesado son inexactos, incompletos o hubieren dejado de ser relevantes o pertinentes para el fin o fines para los cuales hubieran sido registrados, el interesado podrá requerir al responsable del fichero a que ordene que los datos sean rectificados, completados o cancelados, y a que se comuniquen, en su caso, los datos resultantes. 2. La rectificación o cancelación será comunicada, asímismo, a los terceros a los que se hubiera hecho llegar los datos de origen.

[9] Vid. G. GARZÓN CLARIANA. El Proyecto español de ley de protección de datos, en AA.VV. Problemas legislativos... Ob. cit., pp. 135-139, esp. p. 138.

nuestra opinión, y a la vista del esclarecedor artículo citado, era evidente que los datos objeto de cancelación no tenían por qué ser borrados o eliminados de la memoria en la que se guardara el fichero en cuestión, lo cual, por otro lado, era también consecuente con el empleo del término cancelación en el indicado Anteproyecto, ya que, de haberse utilizado los vocablos borrar, eliminar, suprimir, o cualquier otro sinónimo que expresase igualmente este significado, mal hubieran podido ser objeto de conservación, al ser un evidente contrasentido, como pretendían los autores del Anteproyecto.

El Proyecto no recoge ningún precepto similar al indicado pero utiliza hasta la saciedad el término cancelación, presuponiendo de modo preocupante su significado, sin que quede claro en ningún momento su total correspondencia con la idea, aquí sustentada, de eliminación física de los datos almacenados. Esto plantea, a nuestro juicio, la necesidad de poner en marcha una interpretación correctora que sirva para homologar el término con el significado usual que se le otorga a dicha situación jurídica en el Derecho Comparado, y que sea conforme con los Convenios Internacionales suscritos hasta la fecha por nuestro país,[10] pues de otro modo se corre el riesgo de que dicho derecho quede vaciado de contenido en las posteriores reglamentaciones de desarrollo, en las que puede consagrarse sin excesiva dificultad una interpretación en la que se prime la no eliminación o supresión de los datos personales objeto de cancelación –a tenor de los antecedentes a los que hemos hecho referencia no podrá tacharse la misma de totalmente absurda–, e independientemente de que por más que queramos no dejará de contar con numerosos adeptos, tantos como resistentes a su definitiva puesta en práctica puedan existir.[11]

III. LA RELACION DEL DERECHO DE CANCELACION CON OTROS DERECHOS AFINES

El de cancelación guarda una íntima relación con otros derechos que aparecen en las leyes de protección, en especial con los de acceso y de rectificación, participando de la misma naturaleza jurídica que éstos, al ser también un derecho público subjetivo.[12] Estos tres derechos, en realidad, se compor-

[10] En especial, el del Consejo de Europa de 28 de enero de 1981 (ratificado por España mediante Instrumento de 27 de enero de 1984), el cual establece de forma tan clara como contundente que cualquier persona deberá obtener, llegado el caso, la rectificación de sus datos personales obrantes en los ficheros automatizados «... o el borrado de los mismos...» (art. 8. c).

[11] Obviamente existirán esferas que mostrarán una gran renuncia a la operatividad de semejante derecho, y que, ante el silencio del Proyecto o su falta de pronunciamiento en términos incontestables de que cancelación equivale a eliminación física, a destrucción definitiva de los datos almacenados, podrán inclinarse por una interpretación restrictiva del mismo sirviéndose de su significado informático, o incluso, como hemos visto en páginas anteriores, registral, esto es, comportando la conservación indefinida de los mismos.

[12] Según señala el apartado III de la Exposición de Motivos del Proyecto: «las garantías de la persona son los nutrientes nucleares de la Parte General, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en

tan como derechos complementarios entre sí o interdependientes, en la medida en la que su utilización aparece concatenada para garantizar la efectividad del derecho genérico a la libertad informática. En este sentido, para ejercitar la cancelación se hace necesario conocer en profundidad los datos almacenados sobre el interesado en el fichero automatizado, a cuyo fin se prevee el derecho de acceso, cuyo ejercicio previo permite, asimismo, que sean eliminados los datos inexactos o incompletos (art.4.4.). De este modo el derecho de acceso sirve no sólo para poder cancelar o rectificar los datos existentes, sino que cumple además la finalidad de que éstos podrán cancelarse o rectificarse en la medida en la que el ejercicio de dicho derecho se vea oportunamente garantizado. Visto desde este punto de vista el derecho de acceso posee un indiscutible carácter «medial» que no tienen los otros dos restantes derechos con los que aparece ligado por una relación de interdependencia.[13]

Por último, cabe señalar cómo el derecho de cancelación, al suponer el mayor grado de intervención sobre los datos personales existentes en los bancos de datos, al comportar su borrado o supresión, habrá de aparecer rodeado necesariamente de una panoplia de requisitos de mayor rigidez que los que se establecen para los otros derechos existentes en la materia.

IV. SU REGIMEN JURIDICO

El régimen jurídico de la cancelación aparece recogido, fundamentalmente, en los arts. 15, 16 y 17 del Proyecto, aunque los mismos tienen que ser examinados teniendo presentes otros preceptos de la LORTAD.

El apartado primero del artículo 15 del Proyecto remite al reglamento –el recurso a la remisión a la potestad reglamentaria es sumamente frecuente a lo largo de todo su artículado– la determinación del plazo límite que se le marca al responsable del fichero para que cumpla con la obligación de hacer efectivo el derecho de cancelación del interesado. Este precepto plantea la cuestión de si no hubiera sido más acertado el que la propia LORTAD hubiera fijado ella misma un plazo indicativo (mínimo-máximo) para limitar de alguna manera la fijación del mismo por las autoridades administrativas, y ello porque se corre el riesgo de que una cuestión tan importante como ésta acabe convirtiéndose, por la existencia de un cúmulo de plazos diversos, tantos como ficheros o grupos de ficheros quieran establecerse, en un meca-

efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la Parte General, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático».

[13] Los arts. 4.6. y 14 del Proyecto están dedicados a regular el acceso que es definido como el derecho del afectado «a solicitar y obtener información de sus datos personales» (art. 14.1.), datos que, a tenor del art. 4.6. estarán «almacenados de forma que permitan el ejercicio del derecho de acceso».

nismo para ampliar hasta techos temporales inadmisibles los periodos que tienen que esperar los interesados para obtener, llegado el caso, la eliminación de sus datos. Esta posible desviación que puede quedar consagrada en el posterior desarrollo reglamentario viene además agravada por el hecho de que en ningún lugar del Proyecto se señala que dicho plazo tenga que ser unitario para todos los ficheros, y este silencio ha de interpretarse precisamente, no sin un evidente temor, como que se está queriendo dejar una vía abierta para que se fijen múltiples plazos en la materia.

El apartado 2 del artículo 15 plantea, a su vez, la obligación de cancelar los datos inexactos o incompletos una vez que éstos han sido rectificados. Para comprender el sentido de este precepto –de muy poca calidad normativa, dicho sea de paso– ha de interrelacionarse el mismo con el que se recoge en el art. 4.4. conforme al cual se plantea la sustitución de oficio de los datos inexactos o incompletos –que deberán ser, por este motivo, objeto de cancelación (también de oficio), dándose cuenta así del principio de veracidad–, por los correspondientes datos rectificados o completados. De este modo, los autores del Proyecto persiguen que los datos inexactos e incompletos sean eliminados, en aras de satisfacer el indicado principio de veracidad y exactitud, conservándose únicamente los que sea completos y exactos.

Por su parte, el apartado 3 del art. 15 exige la notificación de la cancelación que haya sido efectuada al organismo o entidad a la que haya sido cedido el fichero en el que aparecen los mismos. Con independencia de que aquí sea operativo el art. 19, regulador de los supuestos en los que procede la cesión de datos entre Administraciones públicas, aquella norma no parece satisfactoria, por más que el desarrollo posterior pueda matizarla. En nuestra opinión, ha de hacerse una lectura de la misma a partir de los intereses de los ciudadanos y no de las Administraciones afectadas; esto es, no debería bastar con la notificación al cesionario de que tales o cuales datos han sido eliminados, sino que esta notificación tiene que ser vinculante para el cesionario o cesionarios, pues de otra forma se hace descansar sobre los ciudadanos todo el peso del tráfico informático que las Administraciones pueden llevar a cabo para el mejor cumplimiento de sus fines, obligándolos a cancelar fichero a fichero los mismos datos ya cancelados en el fichero originario, y, pudiendo ocurrir incluso que, por variar la interpretación de las normas existentes por parte de las diversas autoridades administrativas que pueden llegar a ser competentes, en unos casos se produzca este hecho y en otros no. A nuestro juicio debería ser el responsable del fichero originario el que determinara la cancelación para todos ellos sin ningún género de dudas.

A su vez el apartado 4 del artículo que nos ocupa prevee los supuestos en los que no procederá la cancelación, que son dos: *«cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.»*

Ambos supuestos son independientes de aquellos otros en los que se excepciona el ejercicio de los derechos de acceso, rectificación y de cancelación de los afectados, en base a razones de interés público o de intereses de terceros más dignos de protección que, a modo de cláusula de salvaguardia, se recoge en el art. 22.2. del Proyecto.[14]

El primero de los supuestos citados, el que hace referencia a la posibilidad de causar un perjuicio a los intereses legítimos del ciudadano afectado o de terceros, coloca al responsable del fichero en una posición de órgano administrativo tutelante de los intereses privados, sean éstos de la propia persona física afectada o de terceros. Al emplearse conceptos jurídicos indeterminados para describir en qué casos no procederá la cancelación tendrá que ser la propia realidad jurídico-fáctica la que module cuándo nos encontramos ante casos subsumibles en este supuesto normativo, bien entendido que la misma –como también ocurre en los supuestos en los que los datos hayan de conservarse– no puede ser utilizada para interpretar el derecho de cancelación de modo restrictivo.

El segundo hace referencia a la necesidad de mantener los datos por venir a ello obligado el responsable del fichero. Dicha obligación deja de operar, en general, cuando los mismos «hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recogidos» (art. 4.5.), mientras duren los plazos previstos en las disposiciones aplicables, o, en su caso, en las «relaciones contractuales» existentes entre el responsable del fichero y el ciudadano afectado.

La primera de las circunstancias impeditivas de la cancelación se basa en el respeto del principio de conservación, al que, por otro lado, se muestran receptivas todas las leyes de protección de datos –la Data Protection Act inglesa de 1984 lo recoge gráficamente como la conservación de los datos correctos y lícitos–, conforme al cual el mantenimiento de esos datos en dichos bancos de datos resultan imprescindibles para que el mismo sea útil para que las Administraciones Públicas alcancen los fines perseguidos con su creación.

La segunda circunstancia hace referencia al transcurso de los plazos reglamentarios que prevean el mantenimiento de esos datos. Pasados esos plazos no se produce la cancelación de oficio de esos datos, contrariamente a lo que hubiera sido deseable –el Proyecto hace descansar siempre esta operación, salvo que se produzca una rectificación, en el ciudadano afectado–, obligándose únicamente al responsable del fichero a no conservarlo de forma tal que pueda permitir la identificación del interesado (art.4.5.).[15]

---

[14] Y que de invocarse por el órgano administrativo responsable del fichero deberá dictarse por medio de resolución motivada e instruyéndose al ciudadano afectado del derecho que le asiste a poner la negativa en conocimiento del director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de la Comunidades Autónomas.

[15] Señala este precepto lo siguiente: «No serán conservados en forma que permita la

Por último, el precepto en cuestión menciona la posibilidad de que dichos plazos estén previstos en «relaciones contractuales» entre el responsable del fichero y el afectado, esto es, como fruto de todo tipo de convenios, pactos y contratos que pueda mantener la Administración con personas susceptibles de figurar en sus ficheros informáticos.

V. CUESTIONES IRRESUELTAS POR LA LORTAD

El Proyecto deja sin resolver con carácter general y de forma adecuada dos cuestiones que, en nuestra opinión, deberían haber sido abordadas inexcusablemente por vía positiva.

En primer lugar, y por lo que respecta al importantísimo punto de los ficheros manuales, y a las posibles representaciones escritas de los ficheros informáticos –de nada serviría cancelar los datos existentes sí, en paralelo, se mantienen sus expresiones escritas–, el Proyecto, contrariamente a lo que es usual en Derecho Comparado en el que se aborda esta materia como un apéndice necesario de la cancelación, se refiere a él en la Disposición Final Segunda, conforme a la cual el Gobierno «puede» extender las aplicaciones de la Ley, con las adaptaciones que sean necesarias a los ficheros que contengan datos en forma convencional, hayan sido o no sometidos a tratamientos informáticos. A nuestro juicio, y con independencia de que estos ficheros planteen una problemática específica, ligada más que al cumplimiento del art. 18.4. al del art. 105 a) de la Constitución, al acceso de los ciudadanos a los archivos, registros y documentos administrativos –a la que habría de darse un tratamiento normativo adecuado, que por cierto tiene que ser por vía legal, y no reglamentaria (su sede tendría que ser la Ley de Procedimiento Común a la que remite el constituyente)–, los autores de la LORTAD deberían haber hecho referencia puntual a esta cuestión, señalando que en esos casos se produciría también la eliminación física de los datos recogidos en los ficheros manuales. De no ser así se estaría consagrando un mecanismo para el fraude de ley en manos de los funcionarios y de las AA.PP. de las que dependan los ficheros que puede llevar a que todo el esfuerzo del ciudadano para ver eliminados sus datos personales de los ficheros administrativos en los que se encuentran sea simplemente inútil en la práctica, al mantenerse las expresiones escritas de dichos ficheros a pesar de haber sido cancelados los datos que obran en los ficheros informáticos. Dicha vía de fraude que se mantendrá tanto tiempo como el Gobierno tenga a bien tomarse para dar una solución adecuada a este problema.[16]

---

identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos sus valores históricos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos».

[16] El Proyecto de Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, actualmente en tramitación parlamentaria, dedica un extensísimo artículo, el 36, a regular el acceso de los ciudadanos a los archivos y registros administrati-

En segundo lugar, existe otro problema al que no se ha hecho frente de forma adecuada a nuestro juicio: el de la gratuidad o coste de la operación de cancelación. En este sentido lo único que establece el Proyecto es que no se exigirá contraprestación alguna por la cancelación de datos inexactos (art. 16.2.), con lo cual abierta al desarrollo reglamentario posterior la posibilidad de establecer tasas que deberán abonar los ciudadanos si quieren ver cancelados sus datos personales, pues únicamente se prohíbe esta contraprestación cuando se colabora con el principio de veracidad que debe de presidir la redacción del fichero. En nuestra opinión semejante criterio no puede ser aceptado ya que entendemos que la prestación de este «servicio» por la Administración –que no podemos olvidar que no se presta de oficio–, debería ser gratuito, a costa siempre de la Administración que es la que, en última instancia, ha creado el fichero para el cumplimiento de sus fines tanto por lo que se refiere al acceso como para la cancelación de los datos existentes, de conformidad con el criterio que impera en el Derecho comparado más progresivo.

VI. SUPUESTOS DE DENEGACION DE LA CANCELACION DE DATOS

El Proyecto recoge dos supuestos en los que puede denegarse el ejercicio del derecho de cancelación.

El primero hace referencia a los ficheros creados por Fuerzas y Cuerpos de Seguridad los cuales, aparte de tener un régimen particular de cancelaciones (regulado por el art. 20), pueden ver limitado el ejercicio de los derechos de los afectados al acceso, rectificación y cancelación en base a *«los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros, o las necesidades de las investigaciones que se estén realizando»* (art. 21.1.), motivos todos ellos que parecen razonables y justificados.

Asimismo, y por lo que respecta al régimen de cancelaciones en materia de antecedentes policiales y otros datos personales que pudieran obrar en dichos ficheros, el art. 21.4. prevee expresamente la obligación administrativa de cancelar de oficio *«cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento»*, existiendo una serie de circunstancias que de darse motivarán la cancelación de los datos existentes[17].

---

vos, en el que, sin embargo, no se presta atención alguna a este problema de la eliminación de datos obrantes en los mismos. Vid. B.O.C.G.– Congreso de los Diputados. IV Legislatura, Serie A, 4 de marzo de 1992, num. 82-1.

[17] Tales como «la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad».

A diferencia de otros ordenamientos (p. ej., el francés) el nuestro ha rehusado interponer una autoridad administrativa o judicial para que los interesados puedan ejercitar sus derechos en esta materia (el conocido como «acceso indirecto»), pero al propio tiempo ha previsto numerosas circunstancias que pueden hacer inútiles los esfuerzos de los ciudadanos por conocer, rectificar o cancelar sus fichas policiales.[18] Quizás sea por esta razón por la que los redactores del Proyecto han planteado la posibilidad de que los interesados que vean denegado el ejercicio de esos derechos (con base en las circunstancias que se recogen en el citado art. 21.1.) puedan poner en conocimiento del Director de la Agencia de Proteción ese hecho, el cual *«deberá asegurarse de la procedencia o improcedencia de la denegación»* (art. 21.3. in fine).

En segundo lugar, también puede denegarse el ejercicio de ese derecho en el caso de los ficheros fiscales en manos de la Hacienda Pública *«cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras»*, supuesto éste en el que también es posible la intervención del Director de la Agencia de Protección para asegurar la procedencia de la denegación. Ambas circunstancias parecen razonables y justificadas si nos atenemos a los principios de lucha contra la impunidad fiscal que deben de presidir la actuación de la Hacienda Pública.

VII. EL PAPEL DE LA AGENCIA DE PROTECCION EN LA MATERIA

Por último, cabe referirse a los poderes que se le reconocen a la Agencia de Protección de Datos para hacer efectivo el derecho de cancelación, pues entre las competencias de este órgano figura la de *«velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos»* (art. 36 a). Para resolver esta cuestión es imprescindible una referencia al artículo 45, en el cual se preveen una serie de actuaciones que puede poner en marcha la Agencia para el caso de que la autoridad

[18] Para un estudio de esta figura del acceso indirecto, puede verse el trabajo de H. MASI. Etat de la législation francaise et tendeces de la jurisprudence relatives à la protection des données personnelles. Revue Internationale de Droit Comparé, 3, juillet-septembre 1987, pp. 560-580, esp. p. 579. Para un examen de los problemas que, a nivel europeo, plantea este particular sector, vid. G. BUQUICCHIO. «Informática y Libertades: Balance de quince años de actividad del Consejo de Europa», en AA.VV. Jornadas Internacionales... Ob. cit., pp. 97-117, esp. pp. 113-114. Sobre el estado en que se encuentra –inaceptable estado– y la evolución reciente que ha sufrido en nuestro país el uso de la información personal por parte de los servicios policiales puede consultarse el trabajo de M. HEREDERO HIGUERAS: «La Informática y el uso de la informática personal» en A. M. RIVERO-A. SANTODOMINGO (dir.). Introducción a la Informática Jurídica. Madrid, *FUNDESCO*, 1986, pp. 33-46, esp. pp. 39-41.

responsable del fichero no efectúe las oportunas cancelaciones (art. 43.3 f, que lo conceptúa como infracción grave). En ese caso el Director de la Agencia puede dictar una resolución para que cesen o se corrijan los efectos de la infracción (art. 45.1.), pudiendo proponer también la iniciación de actuaciones disciplinarias contra los funcionarios infractores (art. 45.2.).

Estas medidas son excesivamente pobres, algo que, visto desde otro punto de vista, no es sino un botón de muestra de los raquíticos poderes que, a nivel general, se le atribuyen a la Agencia. Y ello por una doble razón, por un lado, porque el acto de la Agencia puede permanecer inejecutado por desidia de la Admninistración respecto a su cumplimiento, y, por otro, porque el incumplimiento repetido del mismo no se soluciona con la mera propuesta –no cabe olvidar que la misma se tendrá que cursar por el conducto reglamentario– de sanciones disciplinarias, máxime cuando los funcionarios son meros ejecutores de la política y las directrices que sobre estos extremos pueden establecer las autoridades políticas y el personal de confianza que es designado por éstas, a las que ni siquiera se refiere el Proyecto.

Todo ello conduce a conformar un panorama en el que el ciudadano que vea «despreciada» su petición de cancelación y acuda a la Agencia para que esta consiga su efectividad, tenga escasas posibilidades de que, salvo que haya «buena voluntad» por parte de la Administración responsable del fichero, tal objetivo se consiga finalmente en vía administrativa sin necesidad de acudir a los Tribunales.

Análisis comparativo entre la Ley 10/1991 portuguesa y el Proyecto LORTAD de nuestro País

M.ª CINTA CASTILLO JIMÉNEZ

Licenciada en Derecho
Profesora de Derecho de la Informática en la Diplomatura de Informática de la Escuela Politécnica de Huelva
(ESPAÑA)

INTRODUCCION

El objeto del presente trabajo es el acercamiento al proyecto de ley orgánica de tratamiento automatizado de datos personales, (LORTAD) español, a través del análisis comparativo con la Ley ya en vigor portuguesa.

El hecho de que el país vecino se haya adelantado, con la aprobación y entrada en vigor de la Ley de protección de datos personales en 1991, nos va a permitir tener elementos de comparación y estudio, entre dos normas con el mismo objeto y finalidad.

Del estudio realizado se desprende que siendo normas parejas, y existiendo una concordancia casi perfecta en cuanto a la forma. El contenido de ambas leyes en ocasiones llega a coincidir perfectamente, otras veces sólo existe un parecido formal y en otros apartados coincidentes por el tema, no tienen nada en común, en cuanto al fondo.

Partiendo de que ambas leyes nacen con la finalidad de regular la automatización de los datos de carácter personal. El análisis pormenorizado de su contenido nos ha permitido observar, que son leyes programáticas que

responden a la necesidad de regulación y protección de parte muy importante de los Derechos de las personas, normas por tanto que dejan buena parte de su contenido esencial y práctico en manos de una posterior regulación reglamentaria.

Lo primero que llama la atención, cuando se comparan ambas normas, es su equivalencia formal, es decir, la concordancia en cuanto a extensión, número de artículos y división temática. Sí bien se dan discordancias en el fondo, a veces de forma absoluta.

La Ley 10/91 de protección de datos personales e informática, portuguesa. Consta de 45 Arts., contenidos en 9 Capítulos, en ellos se incluyen las disposiciones transitorias.

El proyecto de Ley español de LORTAD, está compuesto por 48 Arts. contenidos en 7 Títulos, 3 Disposiciones adicionales, 5 Disposiciones finales, 1 Disposición derogatoria y 1 Disposición final.

Teniendo en cuenta que en el caso de nuestro país, se trata aún de un proyecto de Ley, al que se harán enmiendas, que pueden modificar la estructura final de la norma, en principio ésta es pareja a la de la norma portuguesa.

El Capítulo I de la norma portuguesa y Titulo I del proyecto de LORTAD, coinciden exactamente en cuanto a la forma y estructura, así como en el contenido.

Ambos tratan sobre las disposiciones generales de la norma, con el mismo número de Arts., incluyendo en sus Arts. 1, los principios generales, en los Arts. 2 y 3, el ámbito de aplicación y definiciones imprescindibles dada la novedad y características peculiares de los términos informáticos, que se van a usar en el desarrollo de las normas.

El principio general en el que se funda la norma portuguesa, es imponer el uso transparente de la informática, con un estricto respeto de la vida privada, familiar así como de los Derechos, libertades y garantías fundamentales de los ciudadanos. Añadiendo el proyecto de ley español, que esta norma tendrá como objeto limitar el uso de la informática y otras técnicas, para garantizar todo lo anterior.

El Capitulo II de la norma portuguesa regula la creación, funcionamiento, y competencias de la Comisión Nacional de Protección de Datos Personales Informatizados (CNPDPI).

El sinónimo en el proyecto español, lo encontramos en el Título VI de la LORTAD, que en los Arts. 34 a 41 desarrolla la figura de la Agencia de Protección de Datos.

En ambas normas se tratan los apartados referidos a la creación, funciones y competencias, así como la composición de estos Entes. Si bien en la LORTAD, se hace un desarrollo más exhaustivo de los componentes de la Agencia, así como de la creación de un Registro General, como Organo integrado en la Agencia de Protección de Datos.

La composición de la CNPDPI, portuguesa queda conformada por 7 miembros, de los cuales el presidente y dos vocales, son elegidos por la Asamblea de la República, otros 2 deben ser Magistrados con más de 10 años de ejercicio profesional, 1 Magistrado judicial y otro del Ministerio público. Los otros dos miembros, serán personas de reconocida competencia elegidas por el Gobierno.

En esta composición, y sobre todo en la forma de elección, observamos que se puede dar un predominio claro de las fuerzas políticas mayoritarias en cada momento.

En la LORTAD, no se especifica el número de miembros que formará el Consejo Consultivo, por el que estará asistido el Director de la Agencia de Protección de Datos. Si bien queda perfectamente definida la figura del Director en cuanto a su nombramiento, facultades, consideración de Alto cargo y la plena independencia y objetividad en el ejercicio de sus funciones, como se establece en el apartado 2, del Art.35, y que sinceramente dudamos por la forma en que queda definida en la norma, el nombramiento de éste.

Este se hará a través de un Real Decreto, que será según la experiencia de la trayectoria política reciente de nuestro país, de la tendencia de la mayoría política representada en el Parlamento, y que conforma el gobierno en cada momento.

El Capítulo III de la norma portuguesa, coincide con el Titulo II de la LORTAD, y tratan sobre los principios que deben regir en el procesamiento automatizado de datos personales.

En ellos se desarrolla cómo debe ser la recogida e interconexión de los datos personales, que van a formar parte del fichero automatizado, así como qué tipo de datos pueden ser recogidos y con qué finalidad.

La ley portuguesa establece, las indicaciones que deben aparecer en los documentos que sirvan como base a la recogida de datos.

Nos llama la atención que ahora, la LORTAD empiece a usar el termino «afectado», que define en su Art. 3.c, como persona física titular de los datos que sean objeto del tratamiento automatizado.

Término no muy acertado con el que la LORTAD, intenta definir sin éxito, al titular o persona interesada, más que afectada, que nos puede hacer pensar, en qué estamos afectados de forma negativa, o lo que es igual perjudi-

cados, cuando en realidad desde la norma y ya que se ha hecho una definición previa, se debe desdramatizar y no convertirnos en afectados de antemano.

La norma portuguesa no hace en su glosario de definiciones del Capítulo I, mención alguna a esta figura, porque deben entender que no es necesario definir al propio ciudadano, titular de los datos personales.

En cuanto a los límites de apreciación judicial, la norma portuguesa, establece en su Art. 16, que ninguna decisión judicial, administrativa o disciplinaria puede ser tomada por las autoridades, teniendo como único fundamento el perfil de personalidad del titular del registro del Banco de Datos.

Sobre este perfil de personalidad, resultado del precipitado que combina todos los datos personales y privados de la persona, se establece en el Titulo tercero de la LORTAD, Art. 12, y dentro del reconocimiento de los Derechos de las personas.

«Que el afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea la definición de su personalidad en base al tratamiento automatizado de sus datos de carácter personal.»

Además queda suficientemente definido y avisado su riesgo en el preámbulo de la ley, donde se pone de manifiesto la diferencia entre intimidad y privacidad.

En este sentido, en dicho preámbulo se establece que si bien, está en la mente de todos qué es la intimidad y por tanto el reconocimiento como fundamental del Derecho a la intimidad personal, no está siempre tan claro qué se entiende por privacidad, o en todo caso en qué se diferencia de la intimidad.

Pues bien entendemos, coincidiendo con el preámbulo de LORTAD, que la privacidad constituye un conjunto más amplio de facetas de la personalidad del individuo, que aisladamente consideradas, pueden carecer de significado, pero que coherentemente enlazadas, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene Derecho a mantener reservado, nos estamos refiriendo a datos sobre las enfermedades sufridas en la niñez, el expediente académico, el uso del dinero de plástico, etc.

El conocimiento de estos datos, que combinados dan como resultado un retrato robot, no siempre exacto ni fiable, no es algo nuevo, siempre han estado a nuestro alcance. Sin embargo el tiempo y el espacio jugaban como salvaguarda de la privacidad.

Ahora con las nuevas tecnologías ambas barreras quedan salvadas, en décimas de segundos podemos tener cuanta información deseemos, sin problemas para almacenarla, por tanto es con la aparición de la informática con

lo que aparece también el riesgo de quedarnos desnudos con toda nuestra vida privada al descubierto.

Y lo que es peor corremos el riesgo, si el ordenamiento jurídico no lo impide, de que se hagan perfiles de personalidad sin nuestro conocimiento, ni consentimiento e incluso se nos esté seleccionando para un puesto de trabajo en función a éstos, que pueden basarse como de hecho ocurre en datos erróneos.

En cuanto al acceso a los datos personales, ambas normas contemplan la necesidad de que cualquier persona sea informada de la existencia de los ficheros y Bases de datos, del tipo de datos que tienen recogidos, y de la finalidad y uso que se les van a dar.

El Capítulo IV, de la Ley 10/91 portuguesa, coincide con el Título cuarto de la LORTAD, si bien éste consta de dos capítulos, el primero sobre los ficheros de titularidad pública, y el segundo sobre los ficheros de titularidad privada, esta clasificación por tanto no se contempla en la norma portuguesa.

Sí se recogen los requisitos para la constitución de los ficheros, que deben ser comunicados previamente a la CNPDPI, se recoge en el Art. 19 las indicaciones obligatorias que se deben hacer sobre el fichero, el funcionamiento de éstos, las funciones de sus responsables, y todo lo concerniente a los sistemas de seguridad.

En el Capitulo V, de la ley portuguesa, se trata lo relacionado a la recogida e interconexión de los datos. Esto queda desarrollado en el propio Título cuarto de LORTAD, en ella salvando la distinción entre ficheros públicos y privados, se establece todo lo concerniente a la recogida de datos, la obligación de inscribir los ficheros en el Registro de Protección de Datos. Así como la cesión de éstos, estableciéndose la obligación de que el responsable del fichero informe al interesado, de la cesión, finalidad, nombre y dirección del cesionario, obligación de la que sólo se exime cuando la cesión venga impuesta por Ley.

Aunque como hemos dicho antes, en la norma portuguesa no se establece la clasificación de ficheros públicos y privados en cuanto a la estructura de ésta, se reconoce la distinción cuando en el Art. 25 se cita la interconexión de datos públicos, estableciéndose que pueden ser procesados entre las entidades que persigan los mismos fines. Si bien el Art. 24 establece la prohibición de atribuir un número personal de ciudadano, para la interconexión de ficheros que contengan datos de carácter policial, médico, etc.

El Capítulo VI de la Ley portuguesa, coincide con el Título tercero de la LORTAD, sobre los Derechos y garantías individuales de las personas.

Los Arts. que los conforman suponen un reconocimiento expreso del espíritu que acompaña en todo momento a la norma, y al que debe su razón de ser, y que no es otro que el de proteger al hombre de las posibles violaciones de sus Derechos, en esta ocasión por el uso de las nuevas tecnologías para la automatización de datos personales.

Intentando ambas normas conseguir la convivencia pacífica entre el desarrollo tecnológico, que sin duda nos ha de llevar a un futuro más feliz y la protección de los Derechos por los que tanto se ha luchado, y que ahora corren el riesgo de ser violados. Se trata por tanto de conjugar el fomento de las nuevas tecnologías, protegiéndonos a través de estas normas de posibles ataques a la intimidad, como efectos secundarios del uso de la maravillosa tecnología informática.

El desarrollo de estos Artículos se refiere por tanto al ejercicio del Derecho de acceso a la información, la corrección de datos erróneos, la omisión de datos falsos, así como la inclusión de los que no estén completos.

Todo ello en el caso español, se llevará a cabo por los responsables del Registro General de protección de Datos, que harán posible tanto el acceso a la información, responderán a las consultas de los interesados, y harán las rectificaciones y cancelaciones pertinentes, a instancias de éstos.

La norma portuguesa establece un plazo máximo de 30 días, para que el responsable del fichero dé una respuesta sobre las informaciones inexactas, exigiéndosele la corrección de éstas. Así mismo se puede presentar una queja del responsable de fichero ante la CNPDPI.

El Capítulo VII, de la Ley 10/91 coincide exactamente en cuanto a forma y estructura, y se diferencia muy poco en cuanto a fondo del Título quinto de la LORTAD, tratando sobre el flujo de datos transfronterizos, o movimiento internacional de datos.

Ambas normas exigen autorización de los responsables máximos, en los procesos de automatización de datos personales, en el caso español del Director de la Agencia de Protección de datos, en Portugal se exige así mismo la autorización de la CNPDPI.

En ambos casos también es requisito imprescindible que el país destino, proporcione un nivel de protección equiparable al que prestan estas normas.

Por último ambas leyes definen, la española por inclusión y la portuguesa por defecto, los casos en los que se permitiría la transmisión de datos internacional.

En el caso español, según se recoge en el Art. 33, cuando se apliquen los Tratados o Convenios de los que España sea parte, cuando se solicite auxilio judicial internacional, cuando sean datos de carácter médico que ayu-

den a la investigación epidemiológica, o cuando se trate de transferencias dinerarias según la legislación especifica.

En el caso portugués se establece como decíamos antes por defecto, estableciendo el Art. 33 que queda prohibido el flujo de datos personales a otros países, cuando existan razones fundadas de incumplimiento de la presente Ley. Por tanto en los demás casos entendemos, siempre que existan las garantías suficientes en el país destino, que queda permitido.

El Capítulo VIII de la norma portuguesa coincide en cuanto al tema y estructura con el Título séptimo de la LORTAD, sobre las infracciones y sanciones, sin embargo no existe ninguna coincidencia en cuanto al fondo, es decir en la clasificación de infracciones e imposición de sanciones se siguen regímenes distintos.

La ley 10/91 considera como infracciones de la norma: la utilización ilegal de datos, la obstrucción al acceso de la información contenida en los ficheros, la interconexión ilegal, las informaciones falsas, el acceso indebido o contrario a lo establecido en la norma, la destrucción de datos, la desobediencia de los responsables de los ficheros, etc. Todo ello se castiga con penas de prisión que van desde 120 días a 2 años, pudiendo agravarse en los casos previstos en la ley.

Se aplican así mismo penas accesorias, y se castiga el grado de tentativa en la comisión de estas infracciones o delitos.

En el caso español, la clasificación de infracciones así como las sanciones a imponer siguen el modelo de las cometidas en el ámbito Administrativo, y disciplinario, clasificándose en leves, graves o muy graves.

En cada uno de estos apartados se incluyen los posibles incumplimientos de la norma, estableciéndose una graduación en cuanto a su gravedad.

De la misma forma se establecen las sanciones, en relación a la gravedad determinada por el tipo de infracción, así para las leves se impone una multa pecuniaria que oscila entre 100.000 y 10.000.000 de ptas., las graves, multa de 10.000.000 a 50.000.000 de ptas. y las muy graves, multa desde 50.100.000 a 100.000.000 de ptas.

La cuantía se graduará también en función de la naturaleza de los derechos personales afectados, el volumen de información y los beneficios obtenidos, intencionalidad, reincidencia, etc.

Se establecen en la norma los plazos de prescripción, así como la procedencia del recurso Contencioso-Administrativo, contra las resoluciones de la Agencia de protección de Datos.

En el Capítulo IX de la Ley 10/91 trata sobre las disposiciones transitorias, en cuanto a la obligación de elaborar un Reglamento, los responsables

de los Servicios Públicos que se encargan de los ficheros. Y la legalización de los soportes existentes. Estas disposiciones se recogen en la LORTAD, fuera de los Títulos con numeración aparte y son 3 adicionales, 5 finales, 1 derogatoria y 1 transitoria.

Para concluir, decir que tras este análisis capítulo a capítulo, buscando la equivalencia entre las dos normas, ésta se encuentra fácilmente, pues ambas siguen el mismo patrón en cuanto a estructura, hemos hecho hincapié en aquello que nos ha parecido digno de destacar y sobre todo en lo que no coinciden, pues lo que está claro es que el legislativo español se ha inspirado en la norma portuguesa y en otras ya en vigor para trazar las líneas maestras de la LORTAD.

Todo ello obedeciendo el mandato constitucional, que en su Art. 18.4, establece la Constitución de 1978, de limitar por ley el uso de la informática. Y que 14 años después aún no se ha cumplido, pues la LORTAD, aún no ha visto la luz y puede sufrir muchas modificaciones antes de verla, esperemos que sean en beneficio de todos y que salven los defectos que los expertos han detectado en el aún proyecto de Ley.

Esperamos que sea así pues la LORTAD, supone para muchos la tabla de salvación, que permita conseguir que se conjuguen, desarrollo tecnológico y respeto a los derechos personales del hombre.

Es decir que con una norma adecuada que sirva de límite a los posibles abusos, es como únicamente conseguiremos establecer un equilibrio perfecto entre lo que supone progreso y avance tecnológico y del propio hombre por tanto, y las garantías de respeto absoluto a la vida privada, siendo la norma el instrumento para conseguirlo.

Garantías del ciudadano ante la LORTAD: posibles vías de defensa y protección de sus derechos fundamentales

M.ª EUGENIA GAYO SANTA CECILIA

Abogado
Profesora de la Universidad Nacional de Educación a Distancia (UNED)
Profesora Universitaria en el Colegio Universitario San Pablo CEU de Madrid, División de Derecho
(ESPAÑA)

Con la aprobación por el Pleno del Congreso de los Diputados el pasado 21 de mayo, del *Proyecto de Ley Orgánica reguladora del Tratamiento Automatizado de Datos de carácter personal* (LORTAD), y a falta de su trámite parlamentario en el Senado, parece cercano el ansiado momento de que el derecho español contenga una legislación específica que venga a dar, por fin, cumplimiento al mandato constitucional del art. 18,4 de nuestra Carta Magna.

Con todo, nuestras expectativas en tan anhelada regulación podrían resultar insatisfechas de mantenerse la redacción actual, por cuanto se suponía que con la LORTAD se habría de configurar un específico sistema de garantías frente al uso indebido de los datos personales, y ante su actual contenido dicho sistema puede resultar insuficiente, llegando incluso a rebajar, como más adelante expondremos, el nivel de garantías que existía con anterioridad.

No debemos olvidar que, mediante la regulación contenida en esta norma, ha de venir a darse protección no a cualquier tipo de derechos subjetivos, sino a unos derechos constitucionalmente configurados con el rango de fundamentales, cual son el honor e intimidad personal y familiar, a los que

la propia Constitución otorga una tutela particular, a tenor de lo dispuesto en el art. 53,2. En definitiva, dada la trascendental importancia de los bienes jurídicos que han de ser objeto de protección, parecía que la finalidad había de ser no sólo el que mediante las nuevas tecnologías de la información no pudieran menoscabarse las múltiples facetas que integran la personalidad de un sujeto (su *privacidad*), sino que en caso de producirse dicha lesión el ciudadano pudiera actuar eficazmente en defensa de sus derechos. Desgraciadamente no parece que con la normativa contenida en la LORTAD puedan ser plenamente alcanzados dichos fines.

En favor de la nueva regulación cabe decir que, en principio, parece haberse ajustado casi en su totalidad, a lo dispuesto, tanto en el Convenio de Estrasburgo para la *«protección de las personas con respecto al tratamiento automatizado de datos de carácter personal»* de 28 de enero de 1981, como a lo establecido en la Propuesta de Directiva del Consejo de la Comunidad Europea referida a la *«protección de la persona en el tratamiento de datos personales»*, presentada por la Comisión el 27 de julio de 1990, si bien incurriendo en idéntico grado de generalidad en la redacción de algunos de los preceptos, aspecto justificable en los textos internacionales dado su origen y su finalidad, pero que resulta de difícil aceptación cuando se trata de una norma de derecho interno que viene a desarrollar la cláusula general contenida en el art. 18,4 Const.

Son continuas las remisiones que la ley hace a una posterior regulación por vía reglamentaria, de aspectos tan relevantes como, entre otros, el plazo para cumplir la obligación de rectificación y cancelación de datos (art.15), los procedimientos para ejercitar los derechos de acceso, rectificación y cancelación (art. 16), la interposición de reclamaciones ante la Agencia de Protección de Datos (art. 17), etc, cuestiones todas ellas que se refieren, de forma directa, al sistema de garantía de los derechos fundamentales, por lo que se está dilatando, por tiempo indefinido, el establecimiento de mecanismos concretos que podrán ser utilizados por el ciudadano para exigir de forma efectiva que se salvaguarden sus derechos y libertades afectados por el tratamiento automatizado de datos.

A todo ello hemos de añadir el hecho de que, al realizarse esta futura regulación de los procedimientos de tutela por vía de Reglamento, puede entrañarse el peligro de dejación de aspectos tan esenciales en manos del poder político de turno, lo que podría ir en detrimento del nivel de protección de estos derechos.

Cuestión conflictiva resulta ser también la reiterada utilización de conceptos jurídicos indeterminados, o al menos de difícil precisión (consentimiento, interés general, interés público, etc) que se utilizan en ocasiones para justificar y excepcionar la futura aplicación de la norma, con lo que puede verse mermado el grado de eficacia protectora de la misma. En concreto, al ocuparse el Título Tercero de los denominados *«Derechos de las*

Personas», especialmente en el art. 15 al regular el *«Derecho de rectificación y cancelación»*, se ha obviado el problema de concretar cómo ha de interpretarse este último derecho, por cuando se plantea el problema de que la *«cancelación»* de un dato puede no suponer su completa destrucción física, no implica la eliminación total del dato de un fichero, sino que el registro puede estar provisto de un campo al que se le puede introducir un carácter de cancelación. Con tal operación se estaría indicando que un dato o información no debe ser utilizado, de forma que, en principio dicho dato no vuelve a aparecer al solicitar la información, pero se podría volver a recuperar. Prueba de que esta situación puede llegar a producirse se desprende de la redacción dada al art. 15 en su párrafo 2.º, cuando establece que: *«Los datos de carácter personal que resulten inexactos o incompletos serán cancelados una vez rectificados»*, puesto que si el término cancelación se entiende en el sentido de destrucción o borrado del dato, no parecería necesario tener que proceder a rectificar un dato que se va a hacer desaparecer definitivamente del fichero. Por tanto, el ejercicio de este *«Derecho de cancelación»* al no haberse matizado su alcance, no resulta ser suficiente protección para el ciudadano que puede verse indefenso ante operaciones como la descrita.

Existen en el texto de la ley ciertas normas que si bien en principio parecen venir a instaurar nuevas garantías jurídicas, pueden terminar introduciendo un mayor grado de inseguridad. Nos estamos refiriendo a lo dispuesto en el art. 10 respecto al deber de secreto que obliga, tanto al responsable del fichero como a los demás sujetos intervinientes en el tratamiento de datos, al secreto profesional. Según ello, parece que cuando una persona obligada por dicho precepto, vulnere el secreto profesional, le podrán ser exigidas las correspondientes responsabilidades penales. Sin embargo, curiosamente, si acudimos a nuestro vigente Código Penal nos encontramos con que los preceptos en los que aparece tipificado el delito de revelación de secreto profesional, únicamente resultan de aplicación en el supuesto de abogado y procurador (art. 360 CP) o cuando se trate de funcionario público (arts. 367 y 368 CP), por lo que, de no concurrir dicha condición en el responsable del fichero o personas que realicen el tratamiento de datos, no sería posible utilizar la vía penal para sancionar a los infractores y tutelar los derechos de los ciudadanos, con lo que la supuesta garantía contenida en la LORTAD perdería su virtualidad. Una posible solución que salvaría la precaria situación actual, sería la aprobación de los artículos 194 y 195 del Anteproyecto de Código Penal en su redacción de 30 de diciembre de 1991, puesto que, en ellos se regula con carácter general la apropiación de datos de carácter personal registrados en ficheros y soportes informáticos, así como su difusión y revelación, introduciéndose un tipo agravado si los hechos fueran cometidos por los encargados o responsables de los ficheros. Asimismo, se tipifica el delito de revelación de secretos conocidos por razón del oficio o de las relaciones laborales sin que se fije la concurrencia de ninguna condición especial en los

sujetos que lo cometieren, por lo que se estaría posibilitando la utilización eficaz de la vía penal en los supuestos de incumplimiento del art.10 de la LORTAD. Con todo se trata de una potencial vía de tutela que en un futuro puede llegar a existir de aprobarse el Anteproyecto, puesto que en el momento actual carecemos de semejante posibilidad ante la inexistencia de regulación.

En cuanto al tratamiento específico que la LORTAD contiene en relación a la protección de los derechos de información, acceso, rectificación y cancelación, parece claramente insuficiente, no sólo por dejar en manos de la Agencia de Protección de Datos, un órgano administrativo, la competencia para conocer y resolver de las reclamaciones, pues consideramos que quizás un órgano judicial podría haber resultado más eficaz para resolver los posibles conflictos de intereses que surjan, más aún cuando la actuación ante la que se pretende reclamar ha sido realizada por la propia Administración pública; sino sobre todo por no concretar un procedimiento específico para su resolución. La progresiva burocratización a la que han llegado la mayoría de los órganos administrativos de nuestro país junto a cierta tendencia a la politización de los mismos, no permite que alberguemos excesivas esperanzas ante la creación y funcionamiento de este nuevo ente público.

Con todo se ha introducido una posible intervención de los órganos jurisdiccionales al hacer referencia el art. 17.2 a la hipotética procedencia de un Recurso Contencioso-Administrativo contra las resoluciones de la Agencia de Protección de Datos, si bien surge la duda acerca de a qué tipo de Recurso Contencioso-Administrativo se está haciendo referencia, si al contenido en la Ley Reguladora de la Jurisdicción Contencioso-Administrativa o al regulado en la Ley 62/1978 de 26 de diciembre de protección jurisdiccional de los derechos fundamentales de la persona, ya que, en el caso de que dicho recurso haya de tramitarse por la vía contenciosa ordinaria, la obtención de una resolución definitiva podría prolongarse excesivamente, lo que nuevamente supondría un menoscabo de los derechos y libertades de los ciudadanos.

El mismo resultado se produce en relación al Derecho a ser indemnizado del art. 17.3, tanto por la existencia de una duplicidad de regulaciones según se trate de ejercitarlo ante las Administraciones Públicas o ante sujetos privados, como por la elección de los órganos de la jurisdicción ordinaria como vía de salvaguarda de los derechos en el segundo de los supuestos, puesto que los procedimientos que se pueden instar ante dicha jurisdicción son largos y complejos, lo que podría llegar a desvirtuar la finalidad protectora que se pretende.

Una cuestión que nos parece de extraordinaria importancia, por los peligros que puede entrañar, es la posibilidad que la LORTAD ofrece, de creación de órganos semejantes a la Agencia de Protección de Datos en el ámbito de las diferentes Comunidades Autónomas, así como la existencia en dichos territorios de registros de ficheros sobre materias que sean de su competencia

(Arts. 40 y 41), puesto que no sólo pueden llegar a generarse situaciones de desigualdad jurídica entre los ciudadanos según residan en una Comunidad en la que exista o no dicho órgano de protección, sino que ante situaciones semejantes podrían llegar a dictarse resoluciones diferentes según quien las resolviera.

Como inicialmente mencionábamos, el sistema de garantías fijado en la LORTAD, parece haber venido a restringir el actualmente vigente para la protección del derecho al honor y a la intimidad frente al uso indebido de los sistemas informatizados de tratamiento de datos personales. En el planteamiento de este problema hemos de partir de la previsión constitucional contenida en el artículo 53,2 de la Constitución que establece, la utilización de un procedimiento basado en los principios de preferencia y sumariedad para recabar la tutela de los derechos fundamentales contenidos en la Sección Primera del Capítulo Segundo del Título I del texto constitucional (entre los que se encuentra el derecho al honor e intimidad personal y familiar del art. 18), y si bien es cierto que, en el momento presente no se ha elaborado aún lo que deberá ser la *«Ley de Amparo Judicial Ordinario»* que desarrollará dichos procedimiento preferente y sumario, la doctrina ha venido mayoritariamente entendiendo (interpretación que ha resultado reforzada por lo establecido en la Disposición Transitoria 2.ª, 2 de la *Ley Orgánica 2/1979 de 3 de Octubre del Tribunal Constitucional*, así como en la Disposición Transitoria 2.ª de la *Ley 1/1982 de 5 de mayo reguladora del Derecho al honor, a la intimidad personal y familiar y a la propia imagen*) que hasta en tanto se realice dicha regulación, el mandato del 53,2 queda provisionalmente cumplido, a través de la *Ley 62/1978 de 26 de diciembre de protección jurisdiccional de los derechos fundamentales de la persona*, normativa que instaura una serie de procedimientos que tienen como objeto velar, salvaguardar y garantizar el ejercicio de determinados derechos fundamentales, (entre otros los que se contienen en el art. 18 que quedaron comprendidos en el ámbito de aplicación de la ley en virtud del Real Decreto 342/1979 de 20 de febrero). Concretamente la Ley 62/1978 contempla unas garantías jurisdiccionales diferenciadas para el orden penal, civil y contencioso-administrativo que se caracterizan principalmente por una sustancial reducción de los requisitos exigibles y de los plazos de tramitación de las causas incoadas por los ciudadanos en defensa de sus derechos, por lo que se asegura su protección preferente y sumaria.

Pues bien, con la aparición de la LORTAD, la utilización de la Ley 62/78 como vía de protección de estos derechos parece quedar parcialmente anulada, por cuanto, en virtud de lo dispuesto en la Disposición Derogatoria Unica del Proyecto, a partir del momento de su aprobación, ya no será posible utilizar los mecanismos protectores a los que remitía la Disposición Transitoria 1.ª de la Ley Orgánica 1/1982 de 5 de mayo, es decir, el procedimiento jurisdiccional civil contenido en la ley de 1978, frente a las intromisiones ilegítimas derivadas del uso de la informática.

Una interpretación literal de esta disposición puede conducir a resultados altamente peligrosos ya que, incluso, podría dar lugar a una inconstitucionalidad de la norma por vulneración del mandato del art. 53,2 de la Constitución, dado que el ciudadano se vería imposibilitado, a partir de ese momento, para tutelar de forma preferente y sumaria, sus derechos fundamentales frente al uso indebido de la informática, aunque la propia LORTAD contenga un sistema específico de protección y, cuanto más, porque dicho sistema (al menos en lo que queda esbozado en el Proyecto y sin perjuicio de su posterior desarrollo reglamentario) no parece reunir los caracteres mencionados en el precepto constitucional.

Para evitar que pueda llegar a generarse una situación tan conflictiva como sería una posible declaración de inconstitucionalidad de la ley y, tomando en consideración el principio constitucional de conservación de la norma, proponemos que se mantenga una interpretación en el sentido de entender que la Disposición Derogatoria, únicamente viene a anular la necesidad de acudir a lo dispuesto en la Disposición Transitoria 1ª de la Ley 1/1982 de 5 de mayo, para conocer cuál resulta ser la vía a utilizar para la protección del derecho al honor y a la intimidad frente a la utilización de la informática, pero que ésta sigue siendo la contenida en la ley 62/1978 y, consecuentemente, las menciones que se realizan a lo largo del articulado de la LORTAD a diferentes mecanismos jurisdiccionales (el Recurso contencioso-administrativo del art. 17,2, las acciones ante los órganos de la jurisdicción ordinaria del 17,5) habrá de entenderse que se tramitarán siguiendo las reglas y procedimientos de las Secciones II y III de la Ley 62/78.

CONCLUSIONES

1. La regulación contenida en la LORTAD resulta en algunos puntos, concretamente en el aspecto de las garantías que se le ofrecen al ciudadano para la defensa de sus derechos, claramente insuficientes, llegándose incluso a la necesidad de tener que buscar un sistema de defensa y garantías frente a la propia Ley.

2. Las continuas remisiones que el Proyecto realiza a futuras regulaciones por vía reglamentaria habrán de ser cuidadosamente desarrolladas, so pena de poner en peligro aspectos esenciales de los derechos que se están regulando, lo cual podría llegar a contravenir el mandato que la Constitución hace en su art. 53,1 del respeto al contenido esencial del derecho y, por ende incurrir en inconstitucionalidad.

3. La exclusión del ámbito de aplicación de la LORTAD de las personas jurídicas (según se desprende de la redacción dada a los arts. 1 y 3, e), podría llegar a entrar en contradicción con la normativa penal, de aprobarse el artículo 196 del Anteproyecto de Código Penal de 30-12-1990 que contempla la aplicabilidad de los tipos penales descritos en los arts. 194 y 195

(apropiación y revelación de datos personales) en el caso de datos de las personas jurídicas.

4. En el momento actual no sería posible el empleo de garantías penales para lograr el cumplimiento de lo establecido en la LORTAD, por cuanto en el vigente Código Penal no se contiene ningún tipo penal en el que subsumir dichas situaciones, lo que implica una menor eficacia de aquélla.

5. En relación a las garantías jurisdiccionales civiles y contencioso-administrativas consideramos que deben venir a añadirse a los sistemas de reclamación contemplados en la LORTAD, posibilitándose su utilización por las vías y procedimientos de la Ley 62/78, en aras de garantizar una auténtica protección del derecho al honor y, a la intimidad personal y familiar frente al uso de la informática, así como para mantener en su integridad el sistema constitucional de tutela de los derechos fundamentales.

Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal

GUILLERMO OROZCO PARDO
Licenciado en Derecho
Profesor Titular del dpto. de Derecho Civil de la Univ. de Granada
(ESPAÑA)

El presente trabajo tiene los límites y limitaciones que una comunicación entraña; la materia es extensa, complicada y, sobre todo, muy interesante ya que plantea múltiples problemas y demanda, a veces, soluciones que en técnica jurídica son «arriesgadas». Por ello, abordamos sólo algunas de ellas y, en otros casos, sugerimos posibles puntos de estudio, en la certeza de que la doctrina los estudiará.

I. INTRODUCCION

Las repercusiones sociales de la informática han sido, y serán, de tal magnitud que el Derecho, en cuanto coordinación ética de las relaciones sociales y como técnica de resolución de conflictos, se ha visto compelido a regular y resolver todos aquellos supuestos en los que el uso y abuso de los medios informáticos, ha originado lesiones de distinto orden a los bienes y derechos de las personas. Problemas tales como propiedad del «software», «virus informáticos», delitos perpetrados mediante la informática, etc... son realidades que hoy preocupan a la sociedad y, por tanto, al Derecho. Ello

comporta que el jurista, en sus distintos campos, doctrinal, jurisprudencial y práctico, se vea forzado a tener que dar una respuesta a dichas cuestiones. Como afirma KAISER, el desarrollo de la informática ha suscitado, a la vez que la esperanza de una sociedad mejor informada, más próspera y más libre, serios temores por el mantenimiento del equilibrio de los poderes en las sociedades democráticas, así como por los derechos del hombre y las libertades públicas, se trata de un delicado problema: conciliar el poder estatal, el interés público, con los derechos inviolables de la persona, en base a un espíritu democrático y al Estado de Derecho[1]. Es por ello que nos unimos a las palabras de FROSINI: «Se puede, por consiguiente, comprobar una progresiva "computerización" de la vida privada, no sólo en cuanto se refiere a la cantidad numérica de los individuos fichados, sino también respecto a la particularidad, siempre más detallada y precisa de las informaciones que les conciernen»[2].

El tratamiento legal de la cuestión puede abordarse según distintas técnicas legislativas:

1.ª A través de un enfoque de ámbito constitucional, tal y como sucede en Portugal, Austria o España.

2.ª Los que dispensan un tratamiento globalizador, mediante una Ley General de Protección de Datos, así Francia, Alemania o Suecia.

3.ª Mediante un enfoque de carácter sectorial, dictando normas diferentes para el sector público y el privado, o bien sólo para uno de ellos, como sucede en Estados Unidos o en Dinamarca.

4.ª Por último, un tratamiento específico para temas y actividades concretos, así la Ley Sueca de Información crediticia de 1973.

Es de destacar igualmente el Convenio de Protección de Datos del Consejo de Europa de 28 de Enero de 1981, ratificado por España en 1984, inspirado en las recomendaciones de la OCDE de 1981; así como las dos Propuestas de Directivas de la CEE sobre la materia de 1990.[3] El problema reside en que la solución legal debe evitar la creación de una normativa tan rígida y formalista que impida la existencia y funcionamiento de los bancos de datos, tan útiles en muchos casos. De otro lado, las normas no han de ser

---

[1] Vid. KAISER, P.: *«La protección de la vie privee»*. Ed. Economica, París, 1984, pág. 288. Asi mismo, PÉREZ LUÑO, A. E.: *«Nuevas tecnologías, Sociedad y Derecho»*. FUNDESCO, Madrid, 1987; ORLANDO CASCIO, D.: *«Sulla tutela della riservatezza»*. En: *«Banche datti e diritti della persona»*. Ed. Giuffré, Milano, 1986, págs. 247 y ss y FROSINI, V.: *«Human rights in the computer age»*. En Rv. Informática e Diritto, 1989, págs. 7 y ss.

[2] Vid. FROSINI, V.: *«Cibernética, Derecho y Sociedad»*. Trad. SALGUERO TALAVERA y SORIANO DÍAZ, Técnos, Madrid, 1982, pág. 179. Sobre la multitud de fuentes de recogida de datos, véase Lindon, R. *«Dictionaire juridique: les droits de la personnalité»*. DALLOZ, París, 1983, pág. 123.

[3] Vid. BENAVIDES DEL REY, J. L.: *«Aspectos jurídicos de la protección de datos»*. Rv. Fundesco, n.º 38 de 1984. En el mismo número, véase SANTODOMINGO GARACHANA, A.: *«Una reflexión sobre el anteproyecto de Ley para la Protección de Datos»*, pág. 5 y ss.

tan flexibles e inconcretas que impidan su plena eficacia y aplicación. No se trata, por tanto, de un enfrentamiento o restricción de la informática en cuanto avance esencial de nuestra época, sino de controlar su utilización y sus fines. En definitiva, se trata de disciplinar el fenómeno bajo la perspectiva del control social y democrático de la informática, y de garantizar a la persona su capacidad de decisión y control sobre la existencia, contenido, utilización y fines de los ficheros y bancos que le afectan[4].

De otro lado, nuestra Constitución como otras de su entorno, ya preveía los posibles abusos y peligros que la informática podía generar, por lo que en su artículo 18.4 vincula este fenómeno a contenidos tan elevados como los del Título Primero: los derechos y deberes fundamentales. En concreto, en su Capítulo 2.º, de los derechos y libertades, al ocuparse de derechos fundamentales tan esenciales a la persona como el honor y la intimidad, entre otros, establece en el párrafo 4.º del artículo 18 como una «garantía» de la esfera privada de libertad del individuo y de sus bienes jurídicos tan esenciales como los antes mencionados. A tenor de dicho precepto, «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Este precepto implica un mandato ineludible al legislador para que establezca los mecanismos legales precisos a fin de crear las condiciones necesarias para que tales garantías resulten real y efectivamente aplicables. Castell, al comentar este artículo afirma: «En la mente y en la intención de los autores del 18.4, se denotaba la voluntad, no del todo explícita, de embridar una potente innovación tecnológica, que explotaba por doquier con creciente fuerza», sin embargo, crítica la redacción y alcance del precepto: «La pretensión de establecer garantías de control de los controladores, encubría la falta de alcance de la formula adoptada finalmente»[5]. El precepto liga así la limitación informática al campo individual representado por la «privacy», dejando a un lado afrontarla desde el plano social e institucional, tal y como ha señalado la doctrina, con lo que el tema de la protección de datos no se aborda desde ambos planos cruciales. Sin embargo, existen normas como el artículo 1-b de la Proposición de Ley de Colombia sobre la protección de la «privacy», en la que expresamente se fija como uno de los objetos de la misma «democratizar el poder informático»[6]. Con su ubicación en el artículo 18 se vincula el fenómeno de la informática al campo de los derechos fundamentales de la persona, lo cual tiene como primera consecuencia que la legislación desarrolladora del precepto antes citado habrá de ser por fuerza una Ley Orgánica,

---

[4] Vid. CLARIZIA, R.: *«La proposta del progetto Mirabelli per la tutela della riservatezza»*. En: *«Banchi di Datti e Diritti della Persona»,* CEDAM, Padova, 1985, págs. 128 y ss.

[5] Vid. CASTELL ARTECHE, J. M.: *«La limitación informática»*. En: *«Estudios sobre la Constitución Española»*. H.º a GARCÍA DE ENTERRÍA, coordinador MARTÍN RETORTILLO, Civitas, Madrid, 1991.

[6] Véase el análisis hecho por LOSANO, M. G.: *«Una proposta di legge sulla privacy nella Repubblica di Colombia»*. R. Informática y Diritto, 1988.

con las consecuencias de tramitación y jerarquía que ello conlleva.[7] No obstante, esta afirmación no es unánime en la doctrina pues existen autores como Sempere Rodriguez cuya opinión difiere pues afirma que poniendo en relación los artículos 53.1 y 81 de la CE, la reserva de ley ha de aplicarse sólo a la regulación de los derechos fundamentales y las libertades públicas, es decir, los comprendidos en la Sección 1.ª del Capítulo 2.º del Título 1.º. Como consecuencia de ello dice: «En tanto en cuanto el desarrollo particularizado de los derechos consagrados en el artículo 18 imponga límites al ejercicio de otros derechos, aquellos deberán ser regulados por ley orgánica, pero ello en ningún caso quiere decir que la materia en cuestión, en este supuesto el uso de la informática, deba ser regulado por ley».[8] Sin embargo, el legislador ha planteado la cuestión en sus términos exactos: estamos ante una norma cuyo contenido y finalidad entran de pleno en un campo reservado a regulación por ley orgánica, tal y como expresa el artículo 1 del Proyecto: desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución y «tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos». Mal podría cumplir tales tareas una norma de otro rango, pues su posición jerárquica le obligaría a ceder en determinados conflictos con otros derechos y normas de superior rango, tal y como sería el caso de la libertad de creación, estudio de investigación, práctica médica, etc... (véase el art. 10.7-b del Proyecto). De otro lado, su misión de mecanismo de garantía del pleno ejercicio de los derechos, así como del respeto a los derechos fundamentales, hacen necesario que su rango tenga la «fuerza» suficiente y paralela a tan alta misión. Es por ello que los derechos consagrados en esta Ley pueden entrar en conflicto con las facultades dominicales del propietario de los bienes informáticos, que están limitadas ahora en su ejercicio pues no pueden transgredirse los límites de «privacidad» y fines que el Proyecto consagra. Igualmente sucede con el principio de libertad de empresa: no cabe ya utilizar bancos de datos para almacenar contenidos que puedan suponer discriminación laboral, o contener datos de posibles clientes o que estos no quieran que estén en poder de la empresa. Además, nuestra Constitución recoge la limitación de la informática en su seno como una garantía que los poderes públicos tienen que proporcionar al ciudadano, tal garantía ha de ser respetada por el Estado y los particulares. Todo ello, hace que consideremos adecuado el desarrollo legislativo por vía de la Ley Orgánica, tal y como se ha hecho en el Proyecto, pues de lo contrario poca eficacia

[7] Sobre la cuestión véase la obra de PEMÁN GAVÍN, J.: *«Las Leyes Orgánicas: concepto y posición en el sistema de fuentes del Derecho»*. En *«Estudios sobre la Constitución Española»*. Homenaje al Profesor GARCÍA DE ENTERRÍA». Madrid, Civitas, 1991, Tomo I.

[8] Vid. *«Comentarios a las Leyes Políticas»* EDERSA, Madrid, 1984, Tomo II, pág. 436 y ss.

hubiese podido desplegar, además de obligar a un desarrollo fragmentado y parcial poco adecuado a la importancia del tema.[9]

De otro lado, es interesante resaltar dos cuestiones que la norma plantea:

La primera es la referente al hecho de que, en principio, al tratarse de derechos fundamentales la Ley se aplicará a las personas físicas ya que son estas las que, en puridad de conceptos, son titulares de los bienes jurídicos protegidos por aquellos derechos. Es decir, los datos sensibles cuyo almacenamiento y uso se pretende limitar y regular están referidos a las personas físicas, pero no a las jurídicas. No obstante, puede suceder que alguna de las conductas prohibidas por la norma afecte a personas jurídicas de distinta índole y que estas puedan verse afectadas por ello sin contar con un mecanismo defensivo adecuado a través de esta norma, si bien cabe utilizar la tutela de la acción aquiliana del artículo 1902 del Código Civil en un proceso declarativo ordinario.[10] En atención a ello, se prevé en la Disposición Final Tercera que «el Gobierno, previo informe del Director de la Agencia de Protección de Datos, podrá asimismo extender la aplicación de la presente Ley a los ficheros que contengan datos referentes a las entidades, sociedades y otras personas jurídicas, en las condiciones que reglamentariamente se determinen». Esto no supone que la persona jurídica pase a adquirir la condición de sujeto titular de los derechos y facultades que consagra la norma, pues por esencia ello no es posible, pero para evitar lesiones inadmisibles por indefensión los mecanismos legales, debidamente adaptados, podrán ser extendidos para la protección de tales entidades. Contrasta la postura de la propuesta colombiana, antes reseñada, en el tema ya que el artículo 3-a) de la misma se alude a la tutela de las personas físicas y «personas jurídicas y entes naturales», teniendo estos últimos características comunes con las personas jurídicas, si bien, como señala GUERRERO MATEUS, tales entes no llegan a adquirir personalidad jurídica, pero sin que ello sea obstáculo a crear situaciones jurídicamente relevantes[11].

La segunda cuestión es la relativa a si dentro del ámbito subjetivo de la Ley debemos considerar incluidos, en base al término «ciudadanos», a los nacionales de nuestro país exclusivamente o, por el contrario, también a los

---

[9] No obstante, determinados preceptos del Proyecto tienen carácter de Ley ordinaria en atención a su materia, tal y como establece la Disposición Final 5.ª.

[10] Véase en este sentido VIDAL MARTÍNEZ, J.: *«El derecho a la intimidad en la Ley de 5 de Mayo de 1982»*. Montecorvo, Madrid, 1984, pág. 56 y nota 59; PÉREZ CÁNOVAS, N.: *«Las personas jurídicas y el Derecho al Honor»*. R. F. Derecho de Granada, n.º 15 de 1988, pág. 93 y ss. En el ámbito laboral existe, dentro del deber de buena fe, el llamado «deber de secreto profesional» que veda al trabajador toda conducta de transmisión o difusión de datos concernientes a su empresa que se consideren privados, máxime si conllevan una competencia desleal, ello se consagra en los artículos 72 de la Ley de Contrato de Trabajo y 198 y 499 del Código Penal. Véase ALONSO OLEA, M.: *«Derecho del Trabajo»*. Ed. Un. Complutense, Madrid, 12.ª edición. Lo mismo sucede con los funcionarios en los artículos 367 y 368 del Código Penal.

[11] Véase GUERRERO MATEUS, M.ª F.: *«Osservazioni sulla proposta di legge sulla "privacy" nella Repubblica di Colombia»*. R. I. e Diritto, 1989, pág. 83 y ss.

extranjeros. El término ciudadano hace referencia a la idea de persona, no en cuanto sujeto individual, sino como miembro de una comunidad situado dentro de un marco de relaciones con los demás sujetos. Por ello cuando la CE utiliza el término no lo entiende como sinónimo de «nacional» cuando se está refiriendo a la titularidad de los derechos que son fundamentales en cuanto a su condición de persona, por lo que los extranjeros son tambien sujetos titulares de esos derechos constitucionalmente amparados.[12] En base a ello, debemos considerar que toda persona física es sujeto titular de los derechos consagrados en la presente norma, estando legitimado por ello para ejercitarlo mediante los cauces que reglamentariamente se determinaran, independientemente de su nacionalidad o cualquiera otra condición (así, refugiados, transeúntes, etc....).

Por otra parte, una Ley de estas características se ha de enfrentar a distintos problemas dándole unas soluciones de diversa índole. En primer lugar, debe establecer unos mecanismos de control de los medios informáticos, en segundo lugar, se han de consagrar un conjunto de derechos, de carácter subjetivo y de máxima jerarquía, que la persona puede ejercitar en defensa de su privacidad. De otro lado, deben crearse los mecanismos necesarios para hacer efectivo y eficaz el ejercicio de los mismos, arbitrando las medidas necesarias para sancionar su violación o la obstaculización de éstos.

El problema que nos ocupa se centra en la existencia y transmisión indiscriminada de bancos de datos, públicos y privados, cuyo contenido, titularidad y fines no son conocidos en muchos casos por las personas que en ellos figuran. Datos tan «sensibles» como salud, antecedentes penales, religión, estados civiles, situación económica, filiación política, etcétera, pueden estar almacenados, ser trasmitidos, incluso a título lucrativo, y ser utilizados con fines no siempre lícitos o, cuando menos, desconocidos o perjudiciales para el sujeto.[13]

---

[12] Véase el razonamiento de SEMPERE RODRÍGUEZ en lo relativo a los artículos 13.2 y 23.1 CE en su op. cit.

[13] Tal es el caso de las empresas que con fines comerciales almacenan el contenido de las resoluciones judiciales para elaborar listas en base a criterios de mororisad, sanciones penales, accidentes de tráfico, etc... que luego son vendidas a empresas y entidades bancarias y de seguros, para decidir, por ejemplo, la concesión de créditos o la contratación de trabajadores. Ello motivó que algunos jueces se negaran a facilitar el texto de sus sentencias a tales empresas, alegando el posible mal uso de su almacenamiento, lo cual contradice el esencial principio de publicidad de las mismas, tal y como declaró el Pleno del C. G. P. J. el 30 de Noviembre de 1990. Se trata de crear los mecanismos jurídicos necesarios al ciudadano para acceder y rectificar o cancelar, según el caso, el contenido de esa base de datos en lo referido a su persona. (Vid. diario «El País» de 1 de Diciembre de 1990, pág. 29). Este interesante tema es objeto de estudio por AZPARREN LUCAS, A.: *«Intromisión en el honor e intimidad de las personas por medio de las Sentencias»*. En Actualidad y Derecho, n.º 7 de 1992 donde afirma que *«con carácter general se puede, por tanto, que las sentencias se encuentran exceptuadas por el artículo 8.1 (de la Ley 5 de Mayo de 1982) no pudiendo considerarse ilegítimas las intromisiones al honor o a la intimidad divulgadas por una sentencia»*. En el mismo sentido interpreta el Tribunal Supremo en su sentencia de 16 de Junio de 1989 el artículo 120.1 C. E. pues las resoluciones judiciales se entienden públicas. No obstante, el artículo 906 de la LECrim. permite publicar las sentencias

A tenor de la Constitución, la limitación del uso de la informática pretende evitar dos posibles daños diferentes: la lesión al honor e intimidad personal y familiar y el pleno ejercicio de sus derechos. En lo que a nuestro trabajo se refiere, debemos atender fundamentalmente al bien jurídico de la «intimidad», para precisar inmediatamente que este concepto no es el adecuado para el campo en que nos desenvolvemos, pues hoy la doctrina y el legislador han admitido ya el concepto de «privacidad» de origen anglosajón, («privacy»)[14].

De otro lado, se trata de la consagración a nivel legislativo de un conjunto de derechos subjetivos, referidos a la persona como individuo, como miembro del grupo familiar y como ciudadano, en el seno de los cuales el bien jurídico protegido viene referido a contenidos que afectan a distintos aspectos o esferas de su titular: antecedentes penales, situación familiar, salud, profesión, situación económica, religión, filiación política, etc... y cuyo conocimiento y difusión pueden o no interesar al sujeto o a la sociedad. Lógicamente, se antepone en ciertos casos el interés general como límite al ejercicio de estos derechos, así los datos necesarios para la Hacienda Pública o la Seguridad o Defensa Nacional. En otros supuestos, el almacenamiento de los datos se hace con fines estadísticos o de investigaciones sociológicas; o bien tales datos forman parte de la fase previa a una relación comercial: concesión de un préstamo o expedición de una tarjeta de crédito. El problema no es tanto la existencia de un banco de datos, como el conocimiento que el sujeto tenga del contenido que le afecta, de su veracidad, del grado de privacidad que comporten los datos, y del uso que de los mismos haga el titular de tales bancos.

Las medidas a adoptar, básicamente, han de ser del siguiente orden:

– Un Registro que publique la existencia y finalidad de los bancos de datos, sean públicos o privados, para que su existencia sea conocida por todos, así como su titularidad y fines.

– Unas medidas de control de las personas que pueden tener acceso a tales bancos, sobre todo los que contengan datos «sensibles».

– Un código deontológico para el profesional informático que le dicte una «lex artis» de su profesión, en cuanto imperativo ético de conducta, que

---

suprimiendo los nombres, lugares y circunstancias, e incluso las partes de la misma que puedan ofender a la decencia o atentar a la seguridad jurídica. Por tanto, establecer «bancos parapoliciales de conductas delectivas» de titularidad privada nos parece inadmisible de todo punto, por lo que el archivo informatizado de sentencias habría de realizarse bajo estricto control y, desde luego, sin contener datos de identificación de los sujetos implicados en los asuntos tratados en la sentencia. Incluso el artículo 7.7 de la Ley de 1982 considera intromisión la revelación de datos privados de una persona o familia *conocidos a través de la actividad profesional u oficial de quien las revela»*, conducta ésta que impide facilitar tales datos a profesionales, funcionarios y empresarios con destino a ficheros informatizados.

[14] Se afirma que el origen del término está en la obra de WARREN, S. y BRANDEIS, R.: *«The Right to Privacy»* publicada en Harward Law Review, en 1890. Vid. WACKS, R.: *«The Protection of Privacy»*. London, Sweet & Maxwell, 1980.

consagre una «clausular de conciencia» en la que éstos puedan apoyarse en ciertos casos, así como el deber de secreto, etc...

– La prohibición absoluta de los abusos ocasionados por el «uso desviado» de los datos a fines distintos a los inicialmente previstos y constados. Ello implica la prohibición de las «listas negras» comerciales, laborales, políticas, etc... así como la transmisión comercial de los datos sin consentimiento del sujeto perjudicado.

En el campo concreto de los derechos subjetivos, se trata del reconocimiento de un conjunto formado el derecho de acceso a los ficheros y conocimiento de su contenido, el derecho a obtener la rectificación de su contenido cuando no se ajuste a la realidad, el derecho a la cancelación del contenido cuando éste afecte a datos sensibles que no puedan ser almacenados sino en ciertas circunstancias y el derecho a ser indemnizado por las lesiones que tales abusos puedan producir, para lo cual la norma se remite parcialmente a la legislación penal.

II. PRIVACIDAD E INTIMIDAD

De la lectura del texto se deduce la incorporación al campo jurídico de nuestro país de una serie de términos que, siendo fundamentales para una perfecta comprensión y aplicación de la norma, sin embargo no son fáciles de dotar de contenido exacto. En efecto, palabras como «privacidad» y «datos sensibles» son nuevas en nuestro lenguaje jurídico y, sin embargo, son relevantes a la hora de comprender la norma.

En relación con el término «privacidad», cuyos orígenes han sido comentados anteriormente, su incorporación al texto fue criticada durante el debate parlamentario por considerarse ambiguo y poco definido, ya que pareció mas adecuado mantener el de «intimidad» cuyo contenido y alcance está mas perfilado. En el Derecho Italiano, el término «riservatezza» viene a hacer referencia a la contraposición de intereses entre los sujetos y el almacenamiento y difusión de datos o noticias concernientes a la vida privada de las personas. En el fondo, se trata del interés subyacente del sujeto por conocer y controlar las informaciones que le conciernen, para evitar la difusión de aquellas que pueden ser contrarias a sus intereses, su honor, etc... «es un modo de ser que se contrapone a la publicidad», es un concepto que incluye notas sicológicas y sociales, como dice DE CUPIS es el modo de ser de la persona que consiste en la exclusión de los demás del conocimiento de cuanto hace referencia a la misma persona, es un «modo de ser negativo» de la persona con respecto a los otros sujetos, y más precisamente respecto del conocimiento de éstos. No está referida a su esfera física, sino al orden espiritual que consiste en la exigencia del aislamiento moral, a la no comunicación externa de cuanto atiende a la persona como individuo: es una cualidad

moral de la misma basada en su «derecho a estar sólo».[15] En definitiva, se trata de tener acceso, conocimiento y disposición (control) de lo que Romeo CASABONA llama «identidad informática» para controlar el uso que se realiza de tales datos. Este mismo autor afirma: «Un breve examen de la protección penal de la intimidad en nuestro Derecho revela que aquélla responde a concepciones ya superadas y parcelarias, que resulta insuficiente y, por tanto, insatisfactoria, y mucho más si la vulneración se produce por medios informáticos».[16] De salida, nos parece decisiva la afirmación de Clarizia, en base al proyecto MIRABELLI, de que en una sociedad informatizada la misma noción de intimidad se modifica, pues resulta ya insuficiente.[17] La idea de intimidad personal hace referencia a una esfera de la persona y de su actividad que se sustrae deliberadamente del conocimiento ajeno. Ello le vincula a otras facetas como el honor o la imagen, en cuanto se trata de un ámbito garantizado de la persona frente a intromisiones ilegítimas e inconsentidas por ésta. El propio consentimiento y el ámbito que por la propia conducta se reserva cada persona, son elementos delimitadores del alcance de este derecho, de acuerdo con las normas y usos sociales, lo cual se pone plenamente en evidencia en los casos de colisión con el derecho a transmitir información, tal y como afirma el T.C. en su Sentencia de 5 de Noviembre de 1990, entre otras. En todo caso estamos ante un concepto unitario con distintas manifestaciones, basado en la dignidad de la persona frente a distintos tipos de intromisiones que de una u otra forma afectan a su vida privada, a su honor, etc....[18]. Sin embargo, es importante evitar una indeterminación del concepto lo cual ha sucedido con el término anglosajón «privacy» en cuanto se ha fragmentado su unidad pues se utiliza para hacer referencia a problemas diversos tales como tranquilidad espiritual, derecho al aislamiento, nombre comercial, integridad física o mental, secreto profesional, etcétera, tendientes a reunir toda la gama de derechos y libertades de ámbito individual.[19] En definitiva, ello se conecta con otros términos como «reserva de vida privada», «esfera personal y familiar», que son análogos y pretenden evitar toda una

---

[15] Vid. *«I Diritti della Personalitá»*. En *«Trattato di Diritto Civile e Commerciale»*, de Cicu y Messineo. Milano, Giuffré, Vol. 4.º, 2.ª edición, pág. 283.

[16] Vid. ROMEO CASABONA, C. M.: *«La reforma penal ante las nuevas tecnologías de la información»*. R. I. e Diritto, 1987, pág. 115 ss. Véanse los artículos 194, 195 y 196 del Anteproyecto de Código Penal de 1992 donde se le encuadra dentro de los delitos contra «la intimidad y el secreto de las comunicaciones».

[17] Vid. op. cit. pág. 129; véase también LASARTE ALVAREZ, C.: *«Derecho a la Intimidad "versus" libertad informativa: la primacía constitucional de la intimidad»*, en R. Tapia, n.º 64 de 1992.

[18] No es fácil hacer una clasificación de tales intromisiones, tal y como se deduce de la obra de FARIÑAS MATONI, L.: *«El Derecho a la intimidad»*. Trivium, Madrid, 1983, pág. 7; véase la sistematización que hace ORELLANA ROJAS, G.: *«Informática y derecho a la intimidad»* en las Actas del II Congreso Iberoamericano de Informática y Derecho. Ed. CREI, Guatemala, 1989, pág. 137

[19] Vid. ROBERTSON, A.: *«Privacy and human rights»*. Manchester University Press, 1973 y Belvedere, A.: *«Riservatezza e instrumenti d'informazione»*. En «Dizzionari del Diritto Privatto». Dir. N.Irti, Varese, 1980, Tomo 1, pág. 727.

gama de conductas lesivas contra la esfera privada personal y familiar del sujeto. Tales intromisiones varían desde la intromisión en el domicilio, escuchas telefónicas, violación de correspondencia, divulgación de noticias y cualquier otra forma de perturbación de la «paz doméstica». Se entiende que la privacidad es una necesidad básica, esencial para el desarrollo y mantenimiento de una sociedad libre, así como para la madurez y estabilidad de la personalidad individual. En consecuencia, estamos ante la base para la consagración de un derecho de toda persona frente a las agresiones contra sí mismo, su hogar, su familia, sus relaciones y comunicaciones con los demás, su propiedad y sus negocios. Así concebido, este derecho incluye la protección frente a utilizaciones no autorizadas de su imagen, de su identidad, su nombre o sus documentos personales[20].

En todo caso, es evidente que este derecho posee múltiples matíces que confieren a la persona un amplio ámbito de facultades. De un lado, una posibilidad de excluir a los demás del conocimiento de aquellos aspectos de su vida privada que considere restringidos a su esfera personal o familiar. Este sería el «modo de ser negativo» de que hablaban CARNELUTTI y DE CUPIS. De otra parte, su consentimiento expreso puede ser la razón que legitime el conocimiento o difusión de cualquiera de estos aspectos privados, sobre todo cuando la persona los facilita en el seno de una relación contractual. Sin embargo, como todo derecho posee unas limitaciones que circunscriben su ámbito y modalizan su ejercicio; el interés general representado por distintas razones que permiten unas «inmisiones o intromisiones legítimas»: la seguridad del Estado, la prevención del delito, la investigación y tratamiento sanitarios, etc...[21].

Por otra parte, la jurisprudencia ha consagrado una postura que atiende a la mayor o menor relevancia pública de la actividad o cargo del sujeto, así como a sus hábitos y conducta personal, para establecer los límites de ese ámbito de exclusión del conocimiento de datos de la vida privada.

En relación con la informática, el catálogo de intromisiones podría realizarse en los términos en que lo hace ORELLANA ROJAS señalando una problemática entre informática y derechos en distintos ámbitos:

1.º Aspecto individual:

a– Protección del derecho a la privacidad.

b– Derecho de acceso a los datos (el «habeas data» que citan Nibblett y Tchang-Benoit).

c– Derecho de la persona a ser informada de los datos registrados sobre ella.

---

[20] Vid. Wacks op. cit. pág. y sig.

[21] No obstante, el debate del Proyecto ha puesto de manifiesto lo «discrecional» de tales límites, sobre todo en los bancos de datos policiales y de Hacienda. Véase el diario «El País», 15 de Mayo de 1991, donde algunos juristas tratan esta limitación de anticonstitucional.

d– Derecho de la persona interesada a obtener la rectificación de los datos existentes sobre ella.

e– Derecho a que los datos se utilicen sólo para la finalidad concreta para la que fueron registrados.

f– Derecho a que se cancelen datos cuyo almacenamiento no sea consentido o carezca de legitimidad.

2.º Aspecto institucional o social:

a– Determinación de los gestores de la informática.

b– Posibilidad de informática privada.

c– Control democrático de la informática.

d– Métodos a emplear en la elaboración de las informaciones.

e– Control y Registro de los bancos de datos públicos y privados.

f– Código deontológico de los informáticos.

3.º Aspecto relativo a la protección del individuo frente a los abusos:

a– Organo especializado de la Administración.

b– Comisario Parlamentario, Agencia de Protección de Datos, Defensor del Pueblo.

c– Catálogo de infracciones, sanciones y penas.

d– Protección jurisdiccional.

Como puede verse, las implicaciones y demandas que la materia plantea a nivel legislativo, judicial y administrativo, son múltiples e importantes. A todas ellas pretende dar satisfacción la norma que comentamos, para lo cual parte del mandato constitucional, establecido en los términos que conocemos, pero con plena consciencia de las dificultades que ello ha de solventar. La primera de ellas consiste en que el concepto de intimidad no posee el ámbito objetivo necesario para contener todos los aspectos que la norma pretende proteger. Es por ello que el legislador, en la Exposición de Motivos, aborda la cuestión y nos da las razones por las cuales utiliza ya el termino privacidad.

Tras hacer alusión al mandato de nuestra Constitución, cuya modernidad hace que establezca tales garantías frente a la posible utilización «torticera» de la informática, lo cual tiene su origen en el desarrollo de las técnicas de recolección y almacenamiento de datos que pone a la privacidad ante una potencial amenaza antes desconocida. Dice el texto: «Nótese que se habla de la privacidad, y no de la intimidad: aquélla es más amplia que ésta, pues en tanto que la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo– la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer

de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad en sentido estricto está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la CE y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo». Se trata, por tanto, de un concepto más amplio y globalizador de la esfera personal y familiar, que no se circunscribe a lo que hasta ahora entendíamos por «circulo privado» de la persona, sino de toda una serie de referencias a la misma que sirven para hacer una suerte de «retrato de su personalidad» personal, familiar y social: creencias, religión, salud, taras físicas o psíquicas, comportamientos sexuales, gustos y hábitos de consumo, profesión, propiedades y bienes, deudas pendientes, nivel salarial, nivel cultural y educacional, crédito comercial, etc... entran dentro de ese «supraconcepto» que es fuente de datos de la persona que permiten «retratarle» y obtener información útil para distintas finalidades, sin que el sujeto conozca tan siquiera que tales datos existen y están en posesión de terceras personas o entidades públicas o privadas. En definitiva, nos abonamos a la postura de Alpa en el sentido de que cuando se habla de intimidad, reserva, vida íntima o privada nos estamos refiriendo tan sólo a un aspecto significativo, pero incompleto, del problema. Se entiende que aludimos a las intrusiones en la vida familiar y personal, a la intimidad de las actividades que se desarrollan entre las paredes de la casa, por lo que el daño sólo acontece en la medida en que se viola esta esfera de privacidad, ya sea por publicación de noticias reservadas, sea por difusión de datos personales «e custoditi con cura», o por el uso de las imágenes que se ofrecen al público relativas a aspectos de la vida privada destinadas a permanecer, por su naturaleza, en la intimidad. Por ello, las descripciones y definiciones que hoy se ofrecen sobre la intimidad son parciales y no adecuadas para afrontar el problema en su complejidad. Se trata de elaborar un derecho a la exclusividad del conocimiento de aquello que pertenece a la vida privada, en el sentido de que nadie puede tomar conocimiento ni revelar aquello de esa esfera que el sujeto no quiere que sea conocido por los demás. Se trata de que la persona tenga un poder de control sobre el modo en que las informaciones son recogidas, sobre su contenido y veracidad y sobre el uso que de las mismas puede hacerse[22].

El problema básico estriba en la falta de una figura jurídica netamente perfilada que diera acogida, como bien jurídicamente protegido, a tan complejo contendido. Por ello decía RESCIGNO que la pretensión general de una protección de la persona frente a la «indiscreción», no existía en las legislaciones modernas. «Por lo menos, no existe una fórmula amplia capaz de comprender todas las formas de agresión a la reserva».[23] Esta es la función

[22] Vid. ALPA, G.: *«Compendio del nuovo Diritto Privato»*. UTET, Torino, 1985.
[23] Vid. RESCIGNO, P.: *«Persona e comunità»*. Bologna, 1966.

y contenido del concepto de privacidad y prueba de ello es que actualmente multitud de ordenamientos contienen ya normas legales que la consagran y tutelan.[24] La estructura del término en su origen norteamericano se compone de una doble faceta: «disclosural privacy» e «informational privacy», que tratan de los dos aspectos que reviste el «asalto a la privacidad», la invasión de la esfera privada, la toma y registro de datos, su utilización ilícita y su difusión pública. Como dice RODOTÁ, privacidad significa soledad, aislamiento («el derecho a estar solo»), intimidad, anonimato, reserva, discreción y por ello es un concepto que se proyecta sobre y frente a la colectividad, en el seno de la «aldea global»[25]. Dice ALPA que no se trata de defender al hombre en su fortaleza, «su castillo», no es una cuestión de hermetismo o secreto, ni de asegurar la custodia de un espacio vital, sino de controlar la esfera de reserva que cada uno porta dentro de sí mismo y que aparece «transparentada» e inerme ante los medios y métodos de indagación organizada de los aparatos públicos y privados. Tampoco es posible, por otra parte, el recurso a la privacidad para ocultar datos de carácter económico, patrimonial o penal, impidiendo con ello aquellas formas de control social que tutelan los intereses de la comunidad.

Se trata, por tanto, de la defensa de la persona frente a la intromisión, la recogida, difusión y utilización de aspectos de su vida pertenecientes a su privacidad, actos que hoy son frecuentes y ante los cuales no podía oponerse un conjunto de instrumentos jurídicos eficaces. El aumento de este fenómeno se produce porque, como dice el Proyecto, «las fronteras de la privacidad estaban definidas por el tiempo y el espacio». El primero, procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo así la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban así, como salvaguardia de la privacidad de la persona». El problema es que estos límites han desaparecido hoy, tiempo y espacio no son obstáculo para la informática que puede recoger almacenar, procesar y cruzar datos de muy distinta índole, sea cual sea su lugar y momento de procedencia, sin conocimiento ni consentimiento de la persona afectada. Las posibilidades que ello comporta no escapan al legislador: «Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo debe tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que autorice». Por tanto, el problema no es sólo la recogida y almacenamiento

[24] Así, Estados Unidos, Francia, Gran Bretaña, Italia, Austria, Australia, Japón, entre otros y Textos Internacionales y a nivel de la Comunidad Europea, suscritos ya por nuestro país.

[25] *Rodotá,* St.: *«Alla ricerca delle libertá».* Bologna, 178.1.

ilícito de los datos, sino que el riesgo es aún más grave: «El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor (se basa en la dignidad como afirma Fariñas); y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos». En definitiva, el concepto de privacidad establece una nueva frontera que garantiza aquel ámbito que contiene, para evitar que «un elemento objetivamente provechoso para la Humanidad, no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 CE y al cumplimiento de ese objetivo responde la presente Ley».

III. LOS LLAMADOS DATOS SENSIBLES

Debemos plantearnos ahora cuales son esos «datos sensibles» que dotan de contenido a la privacidad y que lógicamente deben hacer referencia al ámbito de la misma. A tenor de la Doctrina, se entienden por tales, «prima facie», los datos relativos a la salud, vida sexual o convicciones políticas o religiosas, sobre los que no hay obligación de declarar, a tenor del artículo 16.2 CE. No obstante, señala CASTELL, «también se denotaba que datos perfectamente "anodinos" se descubrían de golpe como extraordinariamente sensibles, mediante un simple cambio del fin perseguido, cuestión fácil de llevar a cabo dada la extrema multifuncionalidad de dichos datos».[26] Ello pone de manifiesto que, en muchos casos un dato es inicuo o sensible, no ya por su contenido, sino por el uso que de él se haga, pues como señala el autor citado «la interconexión de ficheros, la libre utilización de los datos, producen la denominada teoría del mosaico (Simitis), por el que datos «a priori» irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionar claves insospechadas sobre una determinada persona». En tal sentido, la postura más lógica, que sostiene la Jurisprudencia alemana, es la de no establecer diferencias entre los datos, atendiendo fundamentalmente al contexto y finalidad con que se utiliza. Por tanto, una norma eficaz ha de atender, no al contenido en concreto del dato desligado de cualquier otro elemento, sino utilizar criterios flexibles adaptables a los supuestos y contextos concretos del caso.

TONIATTI hace unas distinciones partiendo de unos «datos personales irrelevantes o de rutina», sustraídos a este régimen normativo especial. Posteriormente, desde un punto de vista material entiende por datos sensibles «aquellos que más directamente se refieren sea a la esfera personal e íntima,

[26] Vid. CASTELL ARTECHE, J. S.: *«La limitación informática»*. En «Estudios sobre la Constitución Española». cit., pág. 924.

sea a la titularidad de los derechos fundamentales de libertad», en tal sentido, cabe citar creencias religiosas, opiniones políticas, salud, antecedentes penales, origen racial, vida sexual, etcétera. Por último, habla de unos «datos supersensibles o sensibilísimos «para atender a una categoría especial en la que el ordenamiento excluye incluso al propio interesado y el ejercicio de sus medios de control para el acceso, corrección, etc...» Se trata esencialmente de datos personales clasiflicables desde el punto de vista material como datos ordinarios y sensibles que se cualifican ulteriormente por su presencia en archivos destinados a finalidades de orden particular y de valor preeminente, entre los que destacan, en primer lugar, la protección del orden público y de la seguridad nacional y, en segundo lugar, la intimidad en materia sanitaria».[27] Este es el espíritu que subyace en el texto del Convenio de 28 de Enero de 1981, ratificado por España (BOE 15 de Noviembre de 1985), pues además de atender al contenido de los datos, en función de los distintos grados de privacidad, atiende también al control de los métodos y fines de su registro y conservación, estableciendo unas garantías sobre información, acceso, corrección y borrado en favor de la persona afectada.

En definitiva, partimos de una categoría básica de datos sensibles atenientes a las materias ya citadas, si bien la limitación ha de extenderse a los procedimientos, medios y fines del registro de los datos, ya que datos inicuos, en principio, pueden servir para finalidad no admisibles. Por ello, no caben posturas categóricas sobre la cuestión, partiendo de unas materias y bases mínimas, sino que deben emplearse criterios flexibles que se adapten a supuestos concretos en atención a las circunstancias de cada caso.

IV. LAS GARANTIAS

Nos encontramos ahora con otra de las importantes aportaciones que la norma introduce. No se trata ya de meras técnicas limitativas o sancionatorias, sino que el legislador ha querido dar carta de naturaleza a unos derechos subjetivos de carácter personal atribuidos ya a todas las personas físicas. Estamos ante instrumentos que se constituyen en medios de protección y garantía de la privacidad de todo ciudadano frente al abuso informático. En la Exposición de Motivos, el Legislador nos dice ya cuál es la importancia que a tales derechos les confiere la norma: «Las garantías de la persona son los nutrientes nucleares de la Parte General, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación, los que otorgan la virtualidad normativa y

[27] Vid. TONIATTI, R.: *«Libertad informática y Derecho a la protección de los datos personales: principios de legislación comparada»*. Trad. SAINZ AMAIZ, R.V.A.P. n.º 29 de 1991, pág. 139 ss. Véase igualmente MAISL, H., SIMITIS, Sp. y otros: *«Informatique et Droit en Europe»*. Bruxelas, 1985 y Madrid, F.: *«Derecho a la intimidad, Informática y Estado de Derecho»*. Valencia, 1984.

eficacia jurídica a los principios consagrados en la Parte General, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático». Queda patente ya cuál es el rango y la importancia que tales derechos vienen a poseer dentro de nuestro Ordenamiento pues suponen el más eficaz instrumento puesto al servicio del sujeto para la defensa frente a la lesión a la vez que instrumento de control ciudadano, democrático, de la informática en lo relativo a bancos de datos y su utilización. Es más, como dice el Proyecto, tales derechos «se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley». El llamado derecho de acceso tiene incluso plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones públicas, a tenor del artículo 105.b C.E., lo cual hace que la norma lo recoja con toda rotundidad, admitiendo sólo excepciones tales como la seguridad y el cumplimiento de las obligaciones tributarias. En su Título Tercero: «Derechos de las Personas», consagra la norma tales derechos partiendo de la base de su carácter personal, esencial a toda persona física afectada por el tratamiento automatizado de datos que le conciernen, a tenor de lo establecido en el artículo 3, sin olvidar lo que antes dijimos con referencia a las personas jurídicas. La primera cuestión importante estriba en el hecho de establecer la naturaleza jurídica de tales derechos. El legislador, sin más explicaciones, los incluye en la categoría de los derechos subjetivos. Como decía DEL VECCHIO, en todo derecho de este tipo subyace un elemento interno: una posibilidad de querer o hacer, y un elemento externo: una posibilidad de exigir a otros el respeto al mismo.[28] Ese poder, en su doble vertiente, pasa a constituirse como elemento esencial del concepto, por ello decía DE CASTRO que estamos ante «una situación de poder concreto concedida a la persona, como miembro activo de la comunidad jurídica y a cuyo arbitrio se confía su ejercicio y su defensa.[29] En todo caso, la conexión entre derecho subjetivo y libertad se acentúa en las nuevas tendencias pues la teoría de las situaciones jurídicas subjetivas parece haber perdido vigor. No obstante, la vinculación del derecho subjetivo con el concepto de acción en cuanto medio coercitivo de hacer valer en juicio la facultad correspondiente («derecho subjetivo es el que va acompañado de una acción para la realización de las consecuencias jurídicas en caso de violación»), también ha entrado en crisis pues hay derechos y obligaciones que carecen de ella. Como consecuencia de ello se sustituye el concepto de acción por otro más amplio: la garantía jurídica en la que caben distintos medios de protección, como dice CASTÁN, «y que tiene la ventaja de no excluir de la categoría de derechos a los que dimanan de las llamadas obligaciones naturales». Este mismo autor, señala cuáles son los elementos que integran el derecho subjetivo: la voluntad apta del sujeto, que forma el «subs-

[28] Vid. DEL VECCHIO: *«Filosofía del Derecho»*. Ed. española, 1929, pág. 219.

[29] Vid. DE CASTRO Y BRAVO, F.: *«Derecho Civil de España»*. Madrid, Civitas, 2.ª ed. y *«Temas de Derecho Civil»*. Marisal, Madrid, 1972.

trato del derecho», la facultad o poder jurídico, reconocida al titular e integrada por una o varias facultades unidas en un haz o conjunto, sería el «elemento sustancial o contenido» del derecho; tal contenido tiene dos aspectos: la posibilidad de exigir un comportamiento y la posibilidad de obrar válidamente, coinciden con el elemento externo e interno antes comentados. El elemento normativo representado por el ordenamiento que sanciona y protege ese derecho. El interés jurídicamente protegido por ese derecho, que puede ser moral, personal o puramente material o económico. Por último, los medios coactivos de defensa, integrados por las garantías jurídicas puestas al servicio del titular y su derecho, así la acción, excepción, autodefensa, etc...[30] GULLÓN y DÍEZ PICAZO ponen de manifiesto que la idea de derecho subjetivo «implicaba un problema de organización social», pues supone dotar al titular de un ámbito independiente de actuación, lo cual conecta el concepto con la libertad y dignidad, valores fundamentales de la persona, por ello afirman: «Apostar por el derecho subjetivo es apostar por la libertad», frente al intervencionismo estatal, frente al desmesurado crecimiento de los medios técnicos de intromisión en la esfera de libertad y en la privacidad del sujeto, nos encontramos con la figura del derecho subjetivo como ámbito de libre actuación de la persona, como instrumento de su libertad y de su dignidad, por ello dicen: «En cambio, la libertad tiende a ser máxima en el desarrollo de la personalidad, y de ahí la acusada proliferación de los derechos humanos en sus múltiples facetas».[31] Estas palabras cobran especial significado cuando estamos ante derechos subjetivos cuyo objeto está integrado por bienes pertenecientes a la esfera personal o moral del titular, pues en tales casos la conexión derecho-libertad-dignidad está muy acentuada. Cuando estamos ante los llamados bienes esenciales nos referimos a aquellos que atañen a la existencia física o jurídica de la persona, como afirmaba DE CASTRO, en cuanto son imprescindibles para una digna existencia del sujeto. La vida, la integridad, la libertad, el honor o la intimidad son bienes que el sujeto debe tener protegidos por cuanto ello atañe directamente a sus condiciones de existencia, ya sea como individuo (vida) o en cuanto miembro de la comunidad (honor). En función de ello se ha hablado de bienes individuales y sociales de la persona.[32] En base a ello, nos encontramos con unos derechos subjetivos cuyo objeto es extrapatrimonial, referido a elementos o condiciones del titular en cuanto persona, por lo que se adquieren de forma originaria, son esenciales e inherentes a su condición, absolutos, en cuanto exigibles frente a todos, intransmisibles, irrenunciables e imprescriptibles. A partir de esa conexión derecho subjetivo-persona-libertad se puede afirmar que ciertos derechos subjetivos, antes citados, por su condición de inherentes a la persona se confor-

[30] Vid. CASTÁN TOBEÑAS, J.: *«Derecho Civil Español Común y Foral»* Revisada y puesta al día por DE LOS MOZOS, J. L.; Reus, Madrid, 14.ª ed., Tomo I, vol. 2.º.

[31] Vid. GULLÓN BALLESTEROS, A. y DÍEZ PICAZO, L.: *«Sistema de Derecho Civil»*. Técnos, Madrid, 7.ª ed., vol. 1, pág. 433 y ss; igualmente LASARTE en op. cit.

[32] Vid. DE CASTRO: *«Temas...»* cit. loc. cit.

man como el instrumento adecuado para garantizar al individuo una esfera de actuación para el desarrollo de su personalidad, libre de intromisiones o coacciones externas por parte del Estado o los otros miembros de la comunidad. En tal caso, estamos ante derechos básicos que debe poseer toda persona dentro del marco de un Estado de Derecho, de ahí que se les denomine como derechos fundamentales de la persona y en los ordenamientos modernos posean una consagración y tutela de índole constitucional. No obstante, hay que decir que el concepto de derechos fundamentales es moderno pues viene ligado al desarrollo del Estado moderno. La ideología liberal los conceptúa como una esfera de inmunidad frente al Estado que se consagra en la Declaración de los Derechos del Hombre, basada en una óptica iusnaturalista. Pero tales declaraciones son fundamentalmente programáticas, actúan como principios o valores carentes de una eficacia y fuerza de obligar ya que no se incorporan al Derecho positivo. Es preciso pues dar el siguiente paso: incorporarlos a la norma positiva para que puedan realmente desplegar su eficacia y fuerza protectora del sujeto, superándose así el estadio anterior de simples valores programáticos. En esta nueva situación cabe ya entenderlos, según Peces Barba, como «facultad que la norma atribuye de protección a la persona en lo referente a su vida, a su libertad, a la igualdad, a su participación política o social, o a cualquier otro aspecto fundamental que afecte a su desarrollo integral como persona, en una comunidad de hombres libres, exigiendo el respeto de los demás hombres, de los grupos sociales y del Estado y con posibilidad de poner en marcha el aparato coactivo del Estado en caso de infracción».[33] Por tanto, la consagración de tales derechos en los textos constitucionales es definitoria del modelo social que se implanta, pues constituyen la llamada «parte dogmática» de las Constituciones que informa el contenido valorativo del orden constitucional. Por otra parte, frente a la actitud absentista del Estado liberal, el Estado democrático de Derecho ha de adoptar una actitud de promoción y posibilitación de tales derechos, evitando los obstáculos y condicionamientos para el ejercicio y tutela de tales derechos; el Estado viene vinculado por tales derechos, siendo uno de los principios rectores de la política de actuación la promoción y defensa de los mismos. Se ha señalado por la doctrina[34] que nuestra Constitución hace una auténtica declaración de derechos pues el contenido de su Capítulo 2.º, del Título I, «es una concreción del enunciado de valores que expresa en el artículo 1.1». Es decir, que esos valores superiores se concretan posteriormente en el texto constitucional, incorporándolos al Derecho positivo y superando su mera condición programática. Partiendo de un núcleo valor esencial:

---

[33] Vid. PECES BARBA, G.: *«Derechos Fundamentales»*. Madrid, 1976, en lo referente a esta materia nos remitimos a la excelente obra de PÉREZ LUÑO, A. E.: *«Derechos Humanos, Estado de Derecho y Constitución»*. Tecnos, Madrid 3.ª edición, ya que con ella puede obetenerse un completo e interesante conocimiento de la materia.

[34] Vid. SUÁREZ PERTIERRA, G.: *«Comentario introductorio al Capítulo II C. E.»*. En «Comentarios... EDERSA, cit. pág. 268.

libertad e igualdad, se van concretando en toda una serie de derechos y libertades que se constituyen en la base del orden político y la paz social (Cfr. arts 9.2 y 10.1 C.E.). Ese carácter nuclear hace que los derechos fundamentales se caractericen como un componente del orden público pues son «un núcleo indispensable para la convivencia» (SUÁREZ PERTIERRA). La regulación de la materia en nuestra Constitución es moderna y está influida por textos coetáneos como la Constitución Portuguesa, incorporando derechos de nuevo cuño, como medio ambiente, y utilizando un criterio interpretativo flexible que supone la admisión de que los derechos fundamentales son una categoría abierta en la medida en que incorporan los valores esenciales de la comunidad, transcendiendo de su aspecto meramente individual. En tal sentido ha de entenderse la remisión a la Declaración Universal de los Derechos Humanos y los Tratados y Acuerdos ratificados por España sobre tales materias (art.10.2 C.E.), pues se trata de una norma que permite adaptar y «poner al día» a nuestro ordenamiento en atención a la evolución social. El criterio sistematizador que ha seguido la Constitución se basa en la protección que cada uno de ellos recibe: Los derechos que vienen recogidos en el artículo 14 y en la Sección 1ª del capitulo II, son protegidos a través de un procedimiento basado en los principios de preferencia y sumariedad (art. 53.2 C.E.) y, en su caso, del recurso de amparo ante el Tribunal Constitucional (cfr.art. 43 y D.Tr.2ª L.O.T.C.). Los derechos ciudadanos incluidos en la Sección 2ª están protegidos por el recurso de inconstitucionalidad del artículo 161.1 C.E. Se trata de una gradación atenta a la mayor o menor fuerza de protección que se dispensa a tales derechos; la primera Sección tiene una protección reforzada ya que está referida a derechos atribuidos a todos por lo que las garantías protectoras han de ser las más eficaces porque con ello se corresponde con la función que tales derechos cumplen en un Estado Social y de Derecho[35].

No obstante, la doctrina ha planteado la dificultad de aplicar el concepto y estructura del derecho subjetivo a los derechos de la personalidad, así De Castro al abordar la cuestión distingue unos bienes esenciales, vida, integridad personal, libertad, de otros de carácter social, que están referidos a realidades externas de la persona, los cuales poseen una cierta independencia que les acerca a las notas del derecho subjetivo.[36] Frente a ello, autorizadas opiniones consideran que el derecho subjetivo es un concepto técnico jurídico extraído del campo patrimonial lo cual ha hecho que se dificulte su aplicación a figuras más recientes como los derechos de la personalidad. Ese desajuste entre el concepto previo y la categoría posterior no es razón para negar la aplicación del derecho subjetivo como instrumento de técnica jurídica destinado a proteger a la persona y sus bienes materiales e inmateriales. En base

[35] Vid. SUÁREZ PERTIERRA: op. cit.

[36] Vid. DE CASTRO Y BRAVO, F.: *«Los llamados derechos de la personalidad»* A.D. C. 1952, pág. 1263 y ss.

a ello se afirma: «Por ello juzgamos acertada la adopción de la técnica jurídica del derecho subjetivo para la protección de la intimidad de las personas, superando la angosta vía, hasta ahora ofrecida, del artículo 1902 del Código Civil, distinguiéndose esa doble proyección en que se ofrece la intimidad de los seres humanos, en sí mismos considerados, y en sus relaciones con los demás, es decir, como personas, e insertos en el grupo familiar, núcleo entrañable de la vida privada».[37] El Tribunal Constitucional se ha definido ya en el mismo sentido, pues entiende que todo derecho subjetivo cumple una función social dentro del orden de la comunidad, así la propiedad del artículo 33 C.E., nota que se acentúa en estos derechos que constituyen «el fundamento mismo del orden político-jurídico del Estado en su conjunto». Esto se deduce de su «doble carácter», pues en primer lugar, son derechos subjetivos, derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un status jurídico o la libertad en un ámbito de la existencia. Por otra parte, y al propio tiempo, entiende el Alto Tribunal que son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como un marco de convivencia humana justa y pacífica. Esta doble naturaleza se consagra tanto en la Constitución como en los Textos Internacionales y Convenios sobre la materia, como los anteriormente citados. (Cfr. STC 14 de Julio de 1981, entre otras). Desde esta perspectiva, hemos de abordar la configuración jurídica de los derechos que la norma consagra como auténticos derechos subjetivos que vienen a funcionar como garantías de un elemento esencial de la persona: la privacidad, entendida ésta en el sentido antes apuntado, es decir, como bien personal de doble vertiente, íntima y externa, vinculado y tutelado por el derecho fundamental a la intimidad recogido en la Constitución en su artículo 18.1. El titular de estos derechos es la persona física, con las precisiones arriba enunciadas, afectada por el proceso de automatización de datos. Tales derechos se confieren para la defensa de su titular frente a inmisiones o abusos cometidos por medio de la informática: recogida de datos, almacenamiento, transmisión de los mismos e incluso actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o de su personalidad, la llamada «identidad informática». El problema que la norma quiere abordar no es la existencia de bases y ficheros informatizados, sino su descontrol, el desconocimiento de su existencia, los contenidos de los mismos y su utilización ilícita o perjudicial para las personas. Por ello se crea el Registro General de Protección de Datos, dentro de la Agencia de Protección de Datos, en el cual se han de inscribir todos los ficheros de titularidad pública y privada a fin de posibilitar el conocimiento de su existencia y su control por los órganos competentes, así como para que los sujetos puedan ejercitar sus derechos

[37] Vid. VIDAL MARTÍNEZ, J.: *«El derecho a....»* cit. pág. 48 y ss.

frente a ellos. Por tanto, un fichero o base no autorizado e inscrito es, por sí mismo, ilegal y su titular está en una situación de ilicitud, pues al ser oculto no se puede controlar a los efectos que la Ley pretende. Básicamente, la Ley parte de un derecho a la «autodeterminación informática», que se inspira en el principio de que ha de ser el sujeto quien decida qué datos pueden ser almacenados, por quién y para qué fines, lo cual comporta una capacidad de decisión que descansa en una información previa. El eslabón básico y principal del sistema arbitrado por la norma es el derecho de acceso que faculta a su titular para exigir la información precisa de los datos de carácter personal relativos a su persona que se incluyan en un fichero automatizado, se trata del derecho a conocer el contenido de los ficheros automatizados relativo a la esfera personal del titular. El contenido de la información ha de ser completo y exacto, salvo las excepciones que la norma consagra para ciertos temas tales como defensa, seguridad o hacienda. Debe facilitarse mediante consulta visual o escrita, certificada o no, pero siempre en forma legible e inteligible «sin utilizar códigos o claves convencionales que requieran el uso de dispositivos mecánicos específicos», este derecho se puede ejercitar en plazos sucesivos de 12 meses, salvo ciertas excepciones previstas para casos de un «interés especial» del afectado. Si como consecuencia del ejercicio de este derecho, el titular constata que los datos contenidos en el fichero son inexactos, incompletos o han dejado de ser pertinentes o adecuados en atención a la finalidad para la que se registraron, puede exigir bien su rectificación, o que se completen, en ejercicio de su derecho de rectificación. Por otra parte, si tales datos no son pertinentes o adecuados en base a aquella finalidad o relación que originó su registro, o pertenecen a la esfera privada del sujeto en tal grado que éste no desea que se registren, y no viene obligado a permitirlo fuera de los supuestos que la norma establece, podrá ejercitar su derecho de cancelación o de bloqueo exigiendo que se borren o bloqueen tales datos, es decir que desaparezcan del fichero o queden imposibilitados de uso o trasmisión desde el mismo. Como consecuencia de lo anterior, si los datos rectificados o cancelados han sido previamente cedidos, dichas circunstancias seran comunicadas por el responsable del fichero al cesionario para que obre en consecuencia. Así mismo, todo dato personal inexacto o incompleto ha de ser cancelado una vez rectificado, ya que esta circunstancia hace innecesario su mantenimiento. Sin embargo, la norma contiene unas limitaciones a tales derechos, siendo unas más admisibles que otras, sobre todo las que se refieren a ciertos ficheros de titularidad pública como los de policía, defensa o hacienda pública, tal y como consagra el artículo 21, siendo esta la parte más criticable del Proyecto. El derecho de cancelación tiene previstos otras limitaciones en el artículo 15, la primera de ellas tiende a impedir que la cancelación perjudique intereses legítimos de del afectado o de terceros o porque exista obligación de conservar los datos. Vemos difícil que un tercero o «afectado» tenga interés legítimo en que se conserve un dato personal ajeno, y el propio afectado es quien insta la cancelación sabiendo las

consecuencias de ello; el tercero puede ser la Administración, que ya se encarga de asegurarse la mayor discrecionalidad para decidir y limitar estos derechos. Por otra parte, tampoco procede cancelar los datos antes del plazo legalmente establecido para ello en las disposiciones aplicables (¿así los cinco años de Hacienda?) o, en su caso, el plazo previsto en la relación contractual entre el afectado y el responsable del fichero, si bien éste ha de cancelarlos de oficio una vez transcurrido el plazo o extinta la relación contractual, tal y como le exige el artículo 27.2 del Proyecto. En definitiva este derecho a la autodeterminación informática se concreta en unos derechos subjetivos de carácter personal, esencial, indisponible e imprescriptible que se predican de la persona en cuanto tal, y que están concebidos por el Legislador como garantías jurídicas al servicio del derecho fundamental a la privacidad frente al uso de los medios informáticos, lo cual les asimila por su propia naturaleza y función a los llamados «derechos fundamentales de la tercera generación», si bien tienen un caracter instrumental con respecto al derecho constitucional a la intimidad del artículo 18, que se concreta en la privacidad como nuevo contenido «globalizador», tal y como vimos anteriormente.

Ya hemos comentado que el Proyecto contiene aciertos y deméritos suficientes como para merecer un comentario, aunque breve. De salida, la norma en su Titulo Segundo «Principios de la protección de datos» dicta unos mandatos imperativos, a la vez que principios rectores, a los que habrán de atenerse los titulares de los ficheros.[38] En base a ello, cabe entender que los derechos-garantías se han de ejercitar toda vez que se incumplen estos imperativos legales, pero que no es necesario el ejercicio del derecho para que el titular del fichero venga obligado a actuar conforme a la Ley. El artículo 4.1 marca el primer límite: «Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento cuando tales datos sean adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido». Tales conceptos son un tanto inconcretos, pero aplicados al contexto de la norma: la relación entre la persona y el titular del fichero y la finalidad del mismo, permiten una flexibilidad de criterio a la hora de valorar los incumplimientos.

De otro lado, el artículo 4.2 veda el uso de los datos personales objeto de tratamiento automatizado para cualquier uso distinto de la finalidad para la que fueron recogidos. Es decir, tales datos están recogidos para un fin determinado, así investigación médica, contrato de préstamo, tarjeta de crédito, relación laboral, etc... y no pueden utilizarse, ni transmitirse, para otra finalidad diferente a ésta. El párrafo 5.º impone que cuando los datos han dejado de ser necesarios o pertinentes para la finalidad prevista han de ser

[38] Según el artículo 3.a fichero automatizado es «todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso».

cancelados; ello quiere decir, que cuando se extingue la relación preexistente que motivó la recogida, el titular del fichero debe de oficio cancelarlos. Es también importante, el mandato de los párrafos 3 y 4 del artículo citado: los datos han de ser puestos al día de forma que respondan con veracidad a la situación real del afectado. Si tales datos resultan parcial o totalmente inexactos o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados. En todo caso, el almacenamiento de los datos se ha de hacer de forma que permita el ejercicio del derecho de acceso por parte del afectado, lo cual implica la ausencia de claves secretas o archivos ocultos, pues ello es inmediatamente contrario a la norma. La seguridad interna del fichero y la obligación de secreto de las personas relacionadas con el mismo son sancionadas expresamente por la norma en los artículos 9 y 10, su incumplimiento acarrea las sanciones correspondientes, aparte de la responsabilidad frente al afectado.

El conocimiento y consentimiento del sujeto titular de los datos personales es el eje central de la norma y así lo establece como premisa básica el artículo 6: «El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa». Nos movemos dentro del campo de los datos sensibles y supersensibles que antes enunciábamos, por lo que el artículo 16 de la C.E. es un límite a esa posible excepción establecida por la Ley. Es claro que cuando se trate de datos recogidos en instrumentos de acceso al público, Registro de la Propiedad, Mercantil o guía telefónica (Confróntese el artículo 26 del Proyecto), no será preciso el consentimiento, como establece el artículo 6.2 del Proyecto. Ahora bien, el mismo apartado 2 excluye el consentimiento cuando «se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato». Aquí no cabe margen para la discrecionalidad, por lo que hemos de aplicar dos límites: los establecidos en el artículo 4: que sean datos pertinentes, no excesivos y adecuados a la relación y finalidades legítimas del caso, y que cuando dejen de ser precisos o se extinga la relación se cancelen de oficio. En segundo lugar los límites constitucionales del artículo 16 que el Proyecto plasma en su artículo 7 al abordar el tratamiento de los datos supersensibles:

– Nadie puede ser obligado a declarar sobre su ideología, religión o creencias, para el tratamiento de tales datos es imprescindible el consentimiento del afectado, sin excepciones.

– Los datos de origen racial, salud y vida sexual sólo pueden ser recogidos, tratados y trasmitidos con consentimiento del afectado, salvo que prime el interés general o lo disponga una Ley. Realmente, poco interés general debe haber en el origen racial, si no es para discriminar y quebrar el principio

de igualdad. En cuanto a la vida sexual.... no acabamos de entender tal interés. La salud puede ser necesaria para el tratamiento del afectado, prevenir contagios y para la investigación, como dice el artículo 8 del Proyecto, si bien el deber de seguridad y secreto es imprescindible. A nuestro juicio, por la importancia de los bienes protegidos y los serios peligros que puede ocasionar, esta posibilidad discrecional debe interpretarse con criterios muy restrictivos, ya que incluso se duda de su constitucionalidad por algún sector doctrinal[39]. Los ficheros cuya única finalidad sea contener datos supersensibles quedan prohibidos por el artículo 7.4.

– Por último, los datos sobre infracciones penales o administrativas sólo pueden estar en ficheros de titularidad de las Administraciones competentes.

Los derechos subjetivos consagrados por la norma como garantía del derecho fundamental a la intimidad (en su acepción global de privacidad) forman una categoría que se complementa entre sí mismos. El primero de ellos el derecho de información recogido en el artículo 5: «Los afectados a los que se soliciten datos personales tendrán derecho a ser informados de modo preciso e inequívoco:

– de la finalidad y destinatarios de los datos.

– del carácter obligatorio o facultativo de sus respuestas, y de las consecuencias de la obtención de los datos y de su negativa a suministrarlos. En este caso conviene recordar lo antes dicho sobre el artículo 16.2 C.E. y el artículo 7 del Proyecto.

– de la posibilidad de ejercitar sus derechos de acceso, rectificación y cancelación.»

Tales advertencias han de figurar en los cuestionarios, salvo que el carácter de la recogida se deduzca claramente de la naturaleza de los datos o las circunstancias en que se recaban.

No obstante, siembra cierta inquietud pensar en la advertencia de las consecuencias de la negativa a responder, sobre todo en ficheros policiales y de Hacienda, pues estos dos son los supuestos más claros de que entiende el legislador por «interés general», hasta el punto de denegar el ejercicio de los derechos que la Ley reconoce, tal y como sancionan los artículos 19, 20, 21 y 22 del Proyecto, que crean un margen de competencias discrecionales y unas negativas al ejercicio de los derechos, cosa por otra parte lógica, en cuanto se pueden recabar datos supersensibles sin conocimiento, consentimiento y oposición del afectado, razón por la cual se duda muy seriamente de la constitucionalidad de tales preceptos, máxime cuando recordamos que el artículo 19 tiene el carácter de ley ordinaria, y los otros pueden dar pie,

[39] Basta con visionar los cuestionarios psicológicos, vulgo «tests», que se realizan para algunas selecciones de personal y en el servicio militar, para comprender la situación. Véase el diario «El País» del miércoles, 15 de Mayo de 1991.

que no fundamento, a la conculcación de un derecho fundamental e impedir el ejercicio de unos derechos garantías derivados de aquél.

Por otra parte, toda persona tiene derecho a conocer la existencia de ficheros automatizados, de sus finalidades y sus responsables a través del Registro General antes citado, según dispone el artículo 13 como base precisa para poder conocer posteriormente su contenido y obrar en consecuencia, lo cual quiere decir que no es legal el fichero oculto o secreto pues no está debidamente inscrito en el instrumento de publicidad necesario. El derecho de acceso faculta al titular para solicitar y obtener la información al contenido de los datos que le afectan, pudiendo recibirla mediante visualización o por cualquier medio escrito, así copia, certificado, etc... pero siempre en forma inteligible y clara sin que se admitan claves o códigos que precisen dispositivos mecánicos específicos. Este derecho tiene una limitación temporal para su ejercicio: intervalos no inferiores a 12 meses, salvo que se acredite un interés especial. Suponemos que la decisión a hacer consulta visual o solicitar documento o certificado del contenido ha de ser potestativa del afectado, a fin de tener constancia cierta de los datos contenidos y poder ejercitar, si lo estima procedente, los otros derechos que le asisten (art. 14).

Los derechos de bloqueo y cancelación van íntimamente ligados al anterior y su fundamento de ejercicio está en lo que resulte del acceso al contenido del fichero pues si del ejercicio del derecho de acceso resultara que unos datos de carácter personal son inexactos, incompletos o hubieran dejado de ser pertinentes o adecuados para la finalidad para la que hubieran sido registrados, el afectado puede optar por su rectificación, porque se completen, se bloqueen o se cancelen, poniéndosele después de manifiesto los datos resultantes. Luego estamos ante un complejo entramado de facultades de control conferidas al titular: su derecho le faculta a solicitar que se rectifiquen o completen los datos inexactos o incompletos, incluso bloqueando su utilización y transmisión, sin que se pueda exigir contraprestación alguna por los mismos (art. 16.2 Proyecto). Pero si tales datos son inadecuados o han dejado de ser pertinentes puede exigir su cancelación, salvo que ello pueda producir un perjuicio a intereses legítimos del afectado o de terceros o cuando exista la obligación de conservarlos. También se han de conservar durante el plazo establecido en las disposiciones aplicables o en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado. De nuevo estamos ante límites poco precisos, que a nuestro juicio sólo sirven para debilitar las garantías que con tanta firmeza comenta el legislador en su Exposición de Motivos, ya que si son datos supersensibles la cuestión se vuelve mas difícil, sobre todo por lo genérico de expresiones tales como «relaciones contractuales», «disposiciones aplicables», «interés legítimo del afectado o de terceros». Por otra parte, si los datos rectificados o cancelados han sido cedidos, suponemos que con la autorización personal o legal pertinente, el cedente ha de notificar la rectificación o cancelación al cesionario, que vendrá obligado, suponemos, a hacer lo propio, salvo las ex-

cepciones del artículo 19 y siguientes (art. 15 Proyecto). En cuanto al procedimiento de ejercicio de este derecho de acceso, la norma prevé que será establecido reglamentariamente lo cual crea un vacío inadmisible. Como tal derecho subjetivo ligado al derecho fundamental antes citado, debe estar en condiciones de ser ejercitado desde que se apruebe la futura Ley (¡si no antes incluso!) pues no cabe iniciar la aplicación de la norma sin haber previsto paralelamente las condiciones de ejercicio de los derechos que consagra. Si los abusos y lesiones a la privacidad ya existen, debemos de empezar a poner coto a tales conductas por la vía judicial, e incluso a través del Defensor del Pueblo cuando ello sea oportuno. Máxime cuando la Ley establece el derecho a ser indemnizados por los daños y lesiones ocasionados por el incumplimiento de lo dispuesto en ella, atendiendo al régimen de responsabilidad de la Administración para los supuestos de los ficheros de titularidad pública, responsabilidad por el funcionamiento normal o anormal de la Administración; y por los órganos de la jurisdicción ordinaria en los casos de ficheros de titularidad privada. Tales daños, que pueden ser morales y patrimoniales, no pueden quedar hoy impunes por la ausencia de condiciones de ejercicio «reglamentariamente establecidas», por lo que serán, una vez más, los Tribunales los que han de proceder a valorar y sancionar las conductas que conculcan un valor, y un derecho, de tanta importancia como la privacidad en el sentido antes expresado. Parece que el artículo 1902 del Código Civil va a seguir prestando magníficos servicios por ahora, cuando se trata de infracciones de conducta que ocasionen daños por la utilización ilícita de ficheros de titularidad privada. No obstante, conviene recordar que la Disposición Transitoria primera de la Ley de 5 de Mayo de 1982, establece que «en tanto no se promulgue la normativa prevista en el artículo 18, apartado 4.º, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regularán por la presente Ley». Es decir, que el vacío legal existente hasta nuestros días ha sido cubierto por la norma citada, estableciéndose un mecanismo de garantía para estos derechos en tanto no se les dote de una regulación tutelar propia. Sin embargo, el Proyecto pretende derogar esta Transitoria, pero sin establecer paralelamente el mecanismo sustitutivo, pues dice la Disposición Derogatoria: «Queda derogada la Disposición Transitoria primera de la Ley Orgánica 1/1982 de 5 de Mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen». Tal derogación nos parece procedente una vez establecido el cauce adecuado para el ejercicio de los derechos consagrados en la futura LORTAD, pero en el artículo 16.1 el Proyecto se limita a decir: «El procedimiento para ejercitar el derecho de acceso será establecido reglamentariamente», previsión que, sin embargo, puede acarrear una situación de indefensión inadmisible y, como se afirma por la doctrina, posiblemente inconstitucional.

La protección de datos personales en España: presente y futuro

ANTONIO-ENRIQUE PÉREZ LUÑO

Doctor en Derecho por la Universidad de Bolonia
Consejero científico de Informática e Diritto (Florencia)
Miembro del Consejo ejecutivo del Centro de Análisis, Lógica e Informática Jurídica y del Instituto de Derechos Humanos de la Universidad Complutense de Madrid

(ESPAÑA)

1. CRONICA DE UNA PREMONICION CUMPLIDA

El escándalo que en los últimos meses ha agitado a nuestra opinión pública, en relación con el tráfico informatizado de datos de carácter personal, representa la confirmación de un peligro desde hace tiempo anticipado. Los 21 millones de ciudadanos españoles, inmediata o potencialmente, agredidos en su intimidad y otros derechos fundamentales abren una brecha en la inconsciencia cívica y política sobre los peligros que entrañan determinadas manipulaciones de las nuevas tecnologías. Ha sido preciso llegar a esta situación para que el conformismo cotidiano de quienes tienen como misión velar por la tutela de las libertades, y quienes tienen como principal tarea cívica el ejercerlas, se viese agitado por la gravedad del riesgo y la urgencia que reviste su respuesta.

No es lícito, al menos para juristas, políticos y tecnólogos, aducir sorpresa o desconocimiento de los eventuales peligros implícitos en el uso de las nuevas tecnologías. Desde hace tres décadas, quienes han evaluado el impacto de la informática en las libertades, han alertado sobre esos peligros,

y cualquier especialista mínimamente avisado incurriría en negligencia inexcusable de haberlos desatendido. Es cierto que España, aún siendo una sociedad avanzada, dista de los países con tecnología punta. De ahí que, entre nosotros, se juzgara mayoritariamente como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que ahora con el descubrimiento de la red de «piratas» informáticos, se han convertido en una siniestra realidad.

Nuestra sociedad y nuestros poderes públicos permanecieron ajenos e inertes ante una serie de atentados informáticos a la privacidad perpetrados en nuestro entorno político-cultural. Para describirlos no hay que recurrir a una retórica apocalíptica, basta la expresión estricta de un atestado. Desde los años setenta es notorio que bancos de datos del sector público norteamericano, pertenecientes al Pentágono, la CIA o el FBI, procesan informes sobre actitudes individuales y comportamiento político que afectan a millones de ciudadanos. Datos que recabados en función de la defensa nacional o de la seguridad pública han servido, en determinadas ocasiones, para prácticas de control político y discriminación ideológica. La comunidad académica de USA sufrió una conmoción al saber que, durante la etapa de contestación estudiantil, diversas Universidades que contaban con bibliotecas informatizadas porporcionaron a la policía relaciones exhaustivas de las lecturas de aquellos profesores y/o alumnos sospechosos de ser contestarios o disidentes. Desde hace años las agencias de información comercial y de crédito norteamericano almacenan datos personales que conciernen a cientos de millones de individuos, que tras su adecuada programación, pueden transmitirse a sus clientes en más de 10.000 aspectos diferentes (por edad, profesión, sexo, ingresos, automóvil o vivienda poseídos, pertenencia a sindicatos, partidos, o sociedades mercantiles, culturales o recreativas...).

En Francia el detonante fue un proyecto del Instituto Nacional de Estadística, por el que se pretendía atribuir a cada ciudadano un «número de identificación único» para todas sus relaciones con la administración. La fatal coincidencia, para los propugnadores del sistema, de que sus siglas respondieran a la palabra SAFARI, contribuyó a sensibilizar a partidos políticos, medios de comunicación y ciudadanos ante la amenaza de verse convertidos en las piezas a cobrar en el «safari informático». El proyecto fue finalmente suspendido y supuso una eficaz llamada de atención sobre la peligrosidad de las técnicas de over-all computer, o sea, del cruce de ficheros que permiten un control exhaustivo de la población, así como el trazado de un completo perfil de las personas. Estas circunstancias pesaron en 1983 una célebre Sentencia del Tribunal Constitucional de la República Federal de Alemania, que a instancia de los Verdes, declararon parcialmente inconstitucional la Ley del Censo de Población que obligaba a los ciudadanos germanos a suministrar datos personales para fines estadísticos. En dicha decisión jurisprudencial se reconocía el derecho a la «autodeterminación informativa», hasta entonces

invocado por la doctrina jurídica, y concretado en la facultad de todo ciudadano de las sociedades democráticas de determinar: quién, qué, cuándo y con qué motivo puede conocer datos que le conciernen.

No huelga advertir que en nuestro propio país existían también antecedentes inquietantes del actual affaire de la red de piratas informáticos. Desde hace tiempo las instituciones y personas más receptivas a los riesgos de contaminación informática de las libertades han mostrado su preocupación por la persistencia en archivos policiales, ahora informatizados, de datos relativos a actividades políticas, o conductas «desviadas» realizadas en el régimen anterior; el «caso Curiel» constituye un elocuente testimonio. También se han presentado quejas ante el Defensor del Pueblo por la transmisión incontrolada de historias clínicas, así como de datos sobre actitudes y circunstancias personales de funcionarios y trabajadores. Contando con esos notorios antecedentes, patrios y foráneos, mostrar ahora sorpresa resulta una actitud de ignorancia culpable o de cinismo. El tráfico descubierto en estas fechas es el precipitado inevitable de unos riesgos, advertidos desde hace tiempo, y a los que los poderes públicos no han sabido, o querido, poner coto.

2. LAS OPCIONES LEGISLATIVAS DE LA LORTAD

El inquietante panorama español en materia de protección de datos personales exige medidas de urgencia. A ello parece responder el Proyecto de Ley Orgánica para la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal remitida por el Gobierno a las Cortes. (Dicho texto fue publicado en el «Boletín Oficial de las Cortes Generales. Congreso de los Diputados» n.º 59-1, de 4 de Julio de 1991). Conviene indicar que dicho Proyecto llega tarde y mal. Lo primero, porque desde la promulgación de la Constitución, en virtud del expreso mandato de su art. 18.4, así como de la obligación adquirida por la ratificación en 1984 del Convenio de protección de datos personales del Consejo de Europa, el legislador español debía establecer una norma de tutela de las libertades en relación con el uso de la informática. Este compromiso nacional e internacional se ha visto demorado hasta el presente. Lo segundo, porque cabía el consuelo de confiar que nuestro retraso legislativo nos permitiría beneficiarnos de las experiencias previas del Derecho comparado de la informática y evitar sus errores. No ha sido así y el texto remitido a las Cortes presenta algunas deficiencias notables que hay que confiar puedan ser enmendadas en el curso del debate parlamentario previo a su definitiva promulgación.

Para analizar los aspectos más interesantes y polémicos de dicho Proyecto de LORTAD, lo pondré en relación con las grandes opciones legislativas que, en trabajos anteriores, he considerado como informadoras de las normas sobre protección de datos personales:

1) Elección entre un modelo de **ley única y global** (denominada por la doctrina norteamericana Omnibus Act) o por una serie de **leyes particulares**

sectoriales para distintos aspectos de la tecnología de la información y de la comunicación que requieren una reglamentación peculiar (sector by sector en la terminología anglosajona). En este aspecto parece más oportuna una solución mixta, tendente a conjugar una disciplina unitaria con un marco jurídico adaptado a las exigencias de determinados aspectos jurídicos (responsabilidad penal, archivos públicos, datos estadísticos, sanitarios...) o tecnológicos específicos (telecomunicaciones, videotex, transferencia electrónica de fondos...).

La LORTAD parece inclinarse por este sistema mixto, pero no resuelve todos los problemas de concordancias, reiteraciones y antinomias que pueden surgir en este sector de nuestro ordenamiento jurídico. Cuando, por fin, se promulgue la ley de protección de datos su normativa coexistirá con una serie de leyes sectoriales y dispersas (en materia: civil, penal, tributaria, sanitaria, estadística, o de telecomunicaciones) en cuyo articulado se contienen disposiciones sobre el uso de la informática en relación con los derechos fundamentales. Ello puede dar lugar a solapamientos, reiteraciones y contradicciones (antinomias) que deberán ser previstos y evitados. La LORTAD deroga expresamente, en su Disposición derogatoria, la normativa de tutela civil de la intimidad frente a la informática vigente hasta ahora de forma transitoria. También contiene una remisión a la legislación estadística (art.3.d) y sanitaria de protección de datos (arts. 8 y 11.7.b). Pero no se plantea la articulación del régimen de sanciones administrativas previstas en la LORTAD con las sanciones penales que para las infracciones informáticas más graves a la intimidad se prevén en le Proyecto de nuevo Código Penal (art. 194). Tampoco existe alusión expresa a las disposiciones sobre protección de datos personales contenidas en la Ley 30/1984 de Medidas para la Reforma de la Función Pública (art. 13); de la reformada Ley 10/1985 General Tributaria (art. 111.6); y de la Ley 31/1987 de Ordenación de las Telecomunicaciones (arts. 2,2 y 5.4).

La LORTAD debería establecer, por imperativos de seguridad jurídica, una ordenación armonizadora de todas las reglamentaciones sectoriales y dispersas existentes en nuestro ordenamiento en materia de protección de datos. Este tipo de disposiciones han sido denominadas por MARIO G. LOSANO, normae fugitivae, «pues encontrándose allí donde no deberían no son fáciles de hallar, organizando una fuente de problemas legislativos incluso graves».

2) Decisión en favor de textos normativos integrados por **disposiciones casuísticas y pormenorizadas** o por una técnica legislativa de **cláusulas o principios generales.** Este último procedimiento es particularmente aconsejable para regular materias que, como la informática, se hallan inmersas en los constantes cambios e innovaciones tecnológicas. De este modo, la reglamentación legal a partir de unos standards flexibles evita la necesidad de introducir variaciones constantes en las normas y permite a los órganos encargados de su aplicación (tribunales, comisiones, comisarios o agencias...) adaptar los principios a las situaciones que sucesivamente se presenten.

La LORTAD parece querer responder a esa orientación presentándose cono un texto de principios básicos y remitiendo a la vía reglamentaria la concreción de gran parte de su contenido. El desarrollo de esas disposiciones reglamentarias puede suponer una demora adicional en la entrada en vigor de un sistema tutelar eficaz para la protección de las informaciones personales. Sin que puedan tampoco soslayarse las facultades normativas omnímodas y ámpliamente discrecionales que ello comporta en favor de la Agencia de Protección de Datos.

3) Preferencia por un modelo de tutela **«estática»,** basado en la «calidad» de las informaciones, o bien por un sistema de protección **«dinámica»,** centrada en el control de los programas y su utilización. Sobre esta disyuntiva conviene tener presente que la experiencia de estos últimos años sobre la aplicación de las leyes de protección de datos ha puesto de relieve, de un lado, la dificultad de establecer un catálogo exhaustivo de los datos real o potencialmente «sensibles», y de otro, la evidencia de que cualquier información, en principio neutra o irrelevante, puede convertirse en «sensible» a tenor del uso que se haga de la misma, todo ello sin desconocer la importancia que reviste la protección de determinado tipo de datos, en razón de su «calidad», es decir, por su inmediata referencia a la intimidad o el resto de las libertades.

La LORTAD ha optado aquí por una solución sincrética que combina la tutela estática en función de los datos sensibles (art. 7), con la tutela dinámica a través de la Agencia de Protección de Datos (arts. 34 y ss.). Respecto a los primeros hay que reprochar a la LORTAD el haber planteado la tipificación de las informaciones especialmente sensibles en función de la ideología, religión o creencias expresadas en el art. 16 de la Constitución española; cuando resultaba mucho más completo y pertinente haber tomado como punto de referencia el art. 14 de la propia Constitución que previene cualquier actividad discriminatoria –hay que entender que también las realizadas a través de la informática– por razones de «nacimiento, raza, sexo, religión, opinión o cualquier otra circunstancia personal o social».

Respecto a la Agencia de Protección de Datos, ente de Derecho público sobre el que gravita la implementación de la LORTAD y de sus garantías, hay que decir de inmediato que constituye uno de los aspectos más negativos e insatisfactorios del Proyecto. Suscita perplejidad y estupor que la Exposición de Motivos destaque la «absoluta independencia» de su Director y haga hincapié en la «representatividad» del órgano colegiado que le sirve de apoyo. Respecto a lo primero, porque a diferencia de lo que es norma habitual en el Derecho comparado de los Ombudsmen especializados en la protección de datos (el caso de los Datenschutzbeauftragter de las leyes germanas, en las que parece haberse inspirado el Proyecto, es bien elocuente) el Director no es nombrado por el Parlamento, sino por el Gobierno a quien también corresponde su cese (art. 35). Además, a diferencia de los Ombudsmen para la protección de datos extranjeros que presentan sus informes anuales (muy

importantes para conocer el «quién es quién» en materia de agresiones a las libertades informáticas) a las Cámaras representativas, el Director español lo deberá hacer ante el Ministerio de Justicia (art. 36, K). Ello condiciona gravemente la neutralidad y la propia credibilidad de esa institución, que aparece como un mero delegado gubernativo para la informática.

No más indulgente es el juicio que merece la representatividad del órgano colegiado, en el que se incluye una representación empresarial, pero no la de los sindicatos y cuyo procedimiento de elección, tema básico para garantizar la representatividad del órgano, se reenvía a las normas reglamentarias (art. 37).

4) Opción entre restringir la disciplina de los bancos de datos personales a aquellos que pertenecen al **sector público** o extenderla también a los que operan en el **sector privado.** En este punto conviene recordar la admisión paulatina, en la doctrina y la jurisprudencia sobre los derechos fundamentales, del principio de su Drittwirkung, o sea, de su eficacia ante terceros o en relaciones entre particulares. En la fase correspondiente a los derechos de la primera generación se consideraba que éstos sólo eran ejercitables ante los poderes públicos, que tradicionalmente habían sido sus principales violadores. No obstante en las generaciones sucesivas de derechos fundamentales se amplió su incidencia al plano de las relaciones privadas, al adquirirse consciencia de que también en ellas puede surgir situaciones de amenaza y agresión para el disfrute de las libertades. De forma análoga, las leyes de protección de datos de la primera generación tendieron, sobre todo a posibilitar el control de los sistemas automatizados administrativos. Con posterioridad pudo comprobarse que el peligro podía también proceder de los bancos de datos privados (grandes multinacionales, agencias de información y de crédito...) y que urgía evitar situaciones de impunidad para quienes producían este daño a las libertades y de indefensión de quienes son sus víctimas. Ello hace aconsejable una disciplina de todos los bancos de datos personales con independencia de su titularidad pública o privada, introduciendo en la reglamentación aquellas salvedades que se estimen convenientes.

Estas consideraciones pueden también hacerse extensivas a la conveniencia de que la norma de protección de datos haga llegar sus instrumentos de garantía no sólo a los sistemas automatizados, sino también a los archivos o registros manuales referidos a informaciones personales, introduciendo aquí también las eventuales especificaciones.

La LORTAD acoge estas directrices al conjugar la protección de datos personales recogidos en ficheros públicos y privados, estableciendo diferente sistema de garantías. Quizás en este punto la principal objeción que pudiera hacerse al Proyecto es la patente debilidad del sistema de tutela de los bancos de datos privados respecto a los que operan en el sector público. Como he indicado las agresiones de este sector no son menores que las que provienen del poder, por lo que la diferencia de regímenes de protección no tendría

porqué traducirse en merma de los instrumentos de garantía frente a los abusos perpetrados desde la esfera de los grandes intereses económicos privados.

La LORTAD acoge la posibilidad de extender la aplicación de su sistema de garantías a los ficheros convencionales (Disposición final segunda); pero, como en tantos otros puntos, deja al arbitrio del Gobierno, previo informe del Director de la Agencia de Protección de Datos (que como he indicado es un mero delegado gubernativo), la concreción de ese propósito.

5) Delimitación de un ámbito subjetivo de tutela restringido a las personas físicas o ampliado a las personas jurídicas. La primera alternativa es la que cuenta con mayor número de precedentes en el Derecho comparado de la protección de datos. Esto se debe a que, inicialmente, esta legislación fue pensada para proteger la intimidad y las libertades individuales, así como a las dificultades que suponía extender este sistema a las personas jurídicas. Ahora bien, a medida que el proceso de datos se proyecta a las empresas, a las instituciones y asociaciones, se hace cada vez más evidente la conveniencia de no excluir a las personas jurídicas del régimen de protección que impida o repare los daños causados por la utilización indebida de informaciones que les conciernen. En efecto, la defensa de la intimidad y los demás derechos fundamentales no es privativa de los individuos, sino que debe proyectarse a las formaciones sociales en las que los seres humanos desarrollan plenamente su personalidad. De ahí que convergen intereses sociales, jurídicos y políticos en la exigencia de reconocer a las personas colectivas el derecho a la protección de los datos que les conciernan. Todo ello de acuerdo con la tendencia hacia la ampliación de las formas de titularidad que constituyen uno de los rasgos caracterizadores de la tercera generación de derechos fundamentales.

La LORTAD, al igual que en lo concerniente a los ficheros manuales, prevé la posibilidad de extender su sistema de protección, pensado básicamente para las personas físicas, a las jurídicas (Disposición final tercera). Vale aquí también, por tanto, lo apuntado sobre la improcedencia de dejar al arbitrio del Gobierno, previo informe del Director de la Agencia de Protección de Datos, la realización práctica de esta garantía.

3. ¿FICHEROS ROBINSON O FICHEROS PECERA?

Un aspecto de la LORTAD que merece consideración aparte es el referido a sus previsiones normativas para prevenir y sancionar los riesgos que, en orden a la intimidad de los datos personales, se derivan de las prácticas abusivas del correo electrónico y tráfico de datos; peligros que aludía al iniciar estas consideraciones.

Vivimos en una sociedad en la que la información es poder y en la que ese poder se hace decisivo cuando, gracias a la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas.

La información ha devenido símbolo emblemático de una sociedad que se designa a sí misma como sociedad de la información o sociedad informatizada. En esa situación no sería lícito negar a los poderes públicos el empleo de las nuevas tecnologías de la información. En las sociedades avanzadas y complejas del presente la eficacia de la gestión administrativa, la erradicación de actividades antisociales y delictivas cada vez más sofisticadas y la propia moralización de la vida cívica exigen contar con un amplio y organizado sistema informativo. Pero ello no debe implicar que los ciudadanos queden inermes ante el inventario, utilización y transmisión de datos que afecten a su intimidad y al ejercicio de sus derechos.

De modo análogo, en la esfera privada, una vez convertida la información en protagonista del nuevo «sector cuaternario», ahora añadido a los tres sectores económicos tradicionales, se ha desatado la fiebre del acopio de datos. Las sociedades y empresas de hoy miden su dinamismo y empuje por la cantidad y calidad de sus informaciones. La trascendencia económica de la información ha generado un apetito insaciable de obtenerla por cualquier medio y a cualquier precio y es directamente responsable de determinadas prácticas abusivas que hoy, por desgracia, acechan el libre ejercicio de la privacidad de nuestra vida cotidiana.

Para justificar la espiral de datos personales de las agencias de información comercial y financiera se ha llegado incluso a la perversión del lenguaje. Así se alude ahora a los denominados «ficheros Robinson», en los que deberían inscribirse aquellos ciudadanos que no quieran ver perforada su privacidad por la recepción de propaganda no deseada quedando, de este modo, a salvo del mercado «blanco» o «negro» de archivos de información. Ya el nombre de esos ficheros denuncia parcialidad del juicio. Supone que el ciudadano normal es el que acepta gustoso la contaminación de su vida privada por los intereses consumistas de los mercaderes de publicidad. El ciudadano insólito será aquel que se obstine en salvaguardar su derecho fundamental a la intimidad y se autoconfina en un aislamiento parangonable al sufrido por Robinson en su isla solitaria. Podría objetarse a este torpe mensaje ideológico subliminal que precisamente son las sociedades tecnológicas del presente las que han dado origen al fenómeno de las «muchedumbres solitarias» de seres gregarios, espectadores inertes y manipulados por y desde mil formas de propaganda. Todavía es más importante aducir que en un Estado de Derecho ningún ciudadano debe verse obligado a inscribirse en un archivo adicional de datos, para que sean respetados sus derechos y libertades. Parecería grotesco que, en una sociedad democrática, el respeto de la dignidad, de la libertad personal o de conciencia, o el secreto de las comunicaciones quedara limitado a aquellos ciudadanos que expresamente lo solicitasen. Por idéntica inferencia, no deben ser los ciudadanos normales que quieren ejercer su derecho constitucional a la intimidad, sino quienes deseen hacer dejación de este derecho, los que se inscriban en listas o ficheros.

El ciudadano de la sociedad tecnológicamente avanzada sabe que existen los medios para que su formación escolar y universitaria, sus operaciones financieras, su trayectoria profesional, sus hábitos de vida, viajes y esparcimientos, sus preferencias adquisitivas comerciales, su historia clínica, o sus propias creencias religiosas y políticas se hallen exhaustivamente registradas en bancos de datos informatizados susceptibles de ser cruzados, y ofrecer así un perfil completo de la personalidad. Tal situación ha dado origen al denominado «síndrome de la pecera», es decir, la psicosis que aqueja a los ciudadanos de vivir en una casa de cristal en la que todas las acciones pueden ser controladas. Por ello, en aras de la clarificación de las cosas, sería deseable que los ficheros de quienes expresamente no desean ver tutelada su intimidad respecto al tráfico de sus datos personales se denominasen «ficheros pecera», expresión mucho más próxima a su auténtico significado que el equívoco apelativo de «ficheros Robinson».

¿Cuál es la respuesta aportada por la LORTAD para poner coto a esta situación? Vaya por delante que tampoco en este punto el Proyecto se muestra a la altura de las expectativas que su larga y demorada elaboración había generado. En primer lugar, la LORTAD exceptúa del ámbito de su tutela: «A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en Boletines, Diarios o repertorios oficiales» (art. 2.2.c). Asimismo establece que las empresas de recopilación de direcciones, reparto de documentos, publicidad o venta directa sólo utilizarán listas informatizadas de nombres y direcciones de personas físicas cuando figuren en documentos accesibles al público, hayan sido facilitados por los afectados u obtenidas con su consentimiento (art. 29.1). Los interesados podrán ser dados de baja en dichos ficheros tras su expresa solicitud (art. 29.3).

Son varias e importantes las objeciones críticas que pueden argumentarse respecto a ese planteamiento normativo. Me limitaré a exponer las dos que me parecen de mayor entidad. La primera se refiere a que esta disciplina contradice, de manera flagrante, el principio fundamental en la protección de datos de la finalidad (consagrado en el art. 4.2 de la propia LORTAD); ya que no es aceptable que informaciones recabadas y publicadas en función de intereses colectivos y sociales puedan ser incontroladas e impúnemente utilizadas para fines e intereses privados comerciales y, por tanto, ajenos a aquellos que justificaron su recogida y su publicidad. La segunda a que acoge implícitamente la peligrosa y nociva filosofía subyacente a la práctica de los «ficheros Robinson». La LORTAD invierte la carga de la prueba, al exigir del ciudadano que desea ver salvaguardada su vida privada la actuación expresa tendente a la defensa de su derecho, en lugar de hacerla recaer en las empresas que realizan la actividad, las cuales debieran probar que existe un consentimiento previo de cuantas personas figuran en sus bases de datos de información comercial. Todo ello, con el consiguiente riesgo de conculcar la interpretación lógica y sistemática del art. 18 de la Constitución, al implicar

un flagrante e injustificado menoscabo del derecho fundamental a la intimidad.

4. UN RETO INAPLAZABLE

La tardanza en regular la protección de datos personales ha creado ya importantes problemas jurídicos. La demora ha sido culpable de numerosas situaciones de confusión e incertidumbre. Baste mencionar las recientes y sucesivas decisiones discrepantes de juzgados y tribunales y el propio cambio de rumbo del Consejo General del Poder Judicial, en relación con el acceso a las sentencias por parte de agencias de información o entidades financieras, que no persiguen el fin general de la publicidad procesal, sino el de elaborar registros informatizados de morosos o insolventes. Esta cuestión ha sido ahora regulada en la LORTAD, que establece el carácter exclusivamente público de los ficheros de datos personales relativos a infracciones penales o administrativas (art. 7.5), así como las garantías que deberán concurrir en los ficheros automatizados privados sobre datos relativos a solvencia patrimonial y crédito (art. 28).

La nueva ley de protección de datos quizás llegue también tarde para evitar el deslizamiento de nuestro sistema hacia el «identificador único», para cuya fáctica consagración el NIF representó un hito decisivo. Porque no se discute la existencia de documentos que permitan determinar las relaciones del ciudadano con las distintas administraciones, lo que resulta de dudosa constitucionalidad (a la vista del inequívoco propósito, de evitar que en nuestro país se dieran supuestos análogos al «affaire» SAFARI, explicitado por los grupos políticos que contribuyeron a incluir el art. 18.4 en la Constitución) es que esos distintos documentos identificativos consistan en el DNI con un dígito que facilita su procesamiento informático y eventual cruce de ficheros. En este aspecto la única garantía aportada por la LORTAD consiste en limitar la posibilidad de cruce de los ficheros automatizados administrativos. Si bien establece la salvedad de que la cesión «hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso» (art. 19.1).

De lo anteriormente expuesto se infiere que el juicio global que me merece la LORTAD no puede ser positivo. Se me podría objetar que mis reflexiones se han planteado más como un análisis crítico que como una exégesis descriptiva del texto. Lo que es cierto ya que entiendo que, en estos momentos, es todavía posible mejorar el Proyecto, para evitar que al promulgarse la versión definitiva de la LORTAD adolezca de los defectos que ahora tiene, y constituya una lamentable ocasión perdida de dotar a nuestro ordenamiento jurídico de una buena ley de protección de las libertades en la esfera informática. Mi comentario no se consuela con el tópico conformista de que es mejor una ley defectuosa que carecer de cualquier reglamentación legal, entre otras cosas, porque el art. 18.4 de la Constitución y el Convenio Euro-

peo constituyen dos normas básicas vigentes en nuestro ordenamiento, que, aunque exigen un desarrollo legal, ofrecen a la jurisprudencia un cauce orientador mejor que una ley desorientadora y que precariza las principales garantías que dimanan de esos textos. No deseo que mi reflexión pueda pecar de parcialidad, al no reconocer aspectos positivos en la LORTAD. Ahora bien, entiendo que de su articulado pudiera decirse, en síntesis, que sus mayores aciertos residen en aquellos puntos en los que se ha limitado a transcribir garantías existentes en otras normas del Derecho comparado de la protección de datos, en particular del Convenio europeo. Por contra sus aspectos más discutibles e insatisfactorios son, precisamente, aquellos en los que el texto pretende aportar soluciones originales. Entre ellas ocupan un lugar destacado las constantes y significativas excepciones que limitan el alcance práctico del ejercicio de las libertades informáticas. Los constitucionalistas y, en especial, los estudiosos de los derechos fundamentales suelen criticar la práctica desvirtuadora de algunos textos normativos que, tras solemnes y generosos reconocimientos de las libertades, recortan su ejercicio y las vacían de contenido al establecer un régimen de excepciones y limitaciones no menos generoso. Por ello, no puede dejar de suscitar inquietud el que la LORTAD, tras proclamar las garantías en orden a la protección de datos y derechos de las personas, establezca excepciones relevantes referidas a: la información de los afectados (art. 5.3); a su consentimiento (art. 6.1); a las garantías de los datos sensibles (art. 7.3); a la supeditación general de la tutela a cuanto afecte a la Defensa Nacional, Seguridad pública, persecución de infracciones penales o administrativas, interés público o intereses de terceros más dignos de protección (art. 22)... Excepciones que pueden afectar al contenido esencial de la garantía reconocida en el art. 18.4 de la Constitución y sobre la que, por tanto, se cierne la sombra de la inconstitucionalidad.

En las actuales sociedades avanzadas la protección de datos personales tiende, en definitiva, a garantizar el equilibrio de poderes y situaciones que es condición indispensable para el correcto funcionamiento de una comunidad democrática de ciudadanos libres e iguales. Para su logro se precisa un adecuado ordenamiento jurídico de la informática, capaz de armonizar las exigencias de información propias de un Estado avanzado con las garantías de los ciudadanos. Pero estas normas de Derecho informático exigen, para su plena eficacia, impulsar la consciencia y el compromiso cívico de hacerlas una experiencia tangible en la vida cotidiana. Es tarea de todos contribuir a evitar una paradoja dramática: compensar nuestro retraso en la incorporación al desarrollo tecnológico con la vanguardia mundial en la piratería del software, la delincuencia informática, y las agresiones informáticas a la libertad.

BIBLIOGRAFIA

PÉREZ LUÑO, A. E., «Nuevas tecnologías, sociedad y Derecho. El impacto socio-jurídico de las N. T. de la información», *Fundesco*, Madrid, 1987.

PÉREZ LUÑO, A. E., (ed. a cargo de), Problemas actuales de la documentación y la informática jurídica, (Actas del Coloquio Internacional celebrado la Universidad de Sevilla, 5 y 6 de marzo de 1986), Tecnos & Fundación Cultural ENRIQUE LUÑO PEÑA, Madrid, 1987.

PÉREZ LUÑO, A. E., La Contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo, en «Anuario de Derechos Humanos», tomo 4, 1987, Homenaje a JOAQUÍN RUÍZ GIMÉNEZ.

PÉREZ LUÑO, A. E., «Libertad informática y leyes de protección de datos personales», en colab. con M. G. LOSANO y M. F. GUERRERO MATEUS, Centro de Estudios Constitucionales, Madrid. 1989.

PÉREZ LUÑO, A. E., «La incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español», en el n.º 17, monográfico de «ICADE. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales», sobre Informática y Derecho, 1989.

PÉREZ LUÑO, A. E., «Derechos humanos, Estado de Derecho y Constitución», *Tecnos*, Madrid; 4.º ed. 1991.

PÉREZ LUÑO, A. E., «Panorama general de la legislación española sobre protección de datos», en curso de publicación en el vol. col. Implicaciones socio-jurídicas de las tecnologías de la información. Encuentro 1991, *Fundación Citema*, Madrid.

La protección de datos personales en la Península Ibérica

INMACULADA RAMIRO Y LOZANO
Estudiante de Derecho de la Universidad Nacional de Educación a Distancia

VALENTÍN CARRASCOSA LÓPEZ
Doctor en Derecho
Licenciado en Ciencias de la Información
Director del Centro Regional de Extremadura de la Universidad Nacional de Educación a Distancia
Secretario Judicial del Juzgado de 1.ª Instancia e Instrucción n.º 3 de Mérida
(ESPAÑA)

INTRODUCCION

Durante los días 21 a 25 de Septiembre de 1992, tendrá lugar el III CONGRESO IBEROAMERICANO DE INFORMATICA Y DERECHO «NUEVAS TECNOLOGIAS Y LIBERTADES», el cual se celebrará en MERIDA (España), hoy Capital de Extremadura y antaño, Capital de la LUSITANIA ROMANA, bajo la denominación de EMERITA AUGUSTA. En su pasado glorioso, esta Ciudad, con su capitalidad, unificaba gran parte de la Península Ibérica (el suroeste ibérico); pues, LUSITANIA, se componía de lo que hoy es parte del Estado Portugués y parte del Estado Español. Es por ello, que en este emblemático año 1992 queremos aportar lo que se ha hecho sobre «LA PROTECCION DE DATOS PERSONALES EN LA PENINSULA IBERICA».

En nuestro trabajo veremos analogías y diferencias del tratamiento de este tema, en ambos países; traducido en la Ley de Protección de Datos Personales e Informática Portuguesa de abril de 1991 y el Proyecto de Ley Orgánica del Tratamiento Automatizado de los Datos de Carácter Personal de 24 de Julio de 1991 (LORTAD) Español.

Tanto en España como en Portugal, la protección del ciudadano contra los daños causados por el ordenador figura en sus respectivas CONSTITUCIONES.

Si bien, desde el año 1970 en que el Estado de Hesse (República Federal Alemana) publica su célebre: «Ley de Protección de Datos» hasta nuestros días, son numerosos los textos legales dedicados al tema, no es generalizado el hecho de que la Ley Suprema de un País haga referencia a la informática y a la protección de las libertades individuales. (Sin embargo, en la Constitución Austríaca sí se da esta circunstancia). Por ello, la primera analogía encontrada entre estos dos países de la Península Ibérica es el Tratamiento Informático en sus respectivas Leyes Supremas. No obstante, esta identidad entre ambos países ibéricos, tiene distinta redacción en sus Constituciones.

Pero, a pesar de ser un mandato constitucional, no es hasta en esta década de los 90 cuando en Portugal y España se redactan las Leyes de Protección de Datos. Otra analogía, a la que se añadirán a lo largo del trabajo diversas diferencias. La primera de ellas es el porqué del nacimiento de dichas leyes.

En el caso Portugués, la Lei num. 10/91 «Lei da PROTECÇAO DE DADOS PESOAIS FACE INFORMATICA», nace como consecuencia de una Sentencia del Tribunal Constitucional Portugués, la registrada como «ACORDAO núm. 182/87».

El proyecto de LORTAD español nace por iniciativa del Gobierno. Este proyecto de ley fue elaborado por el Ejecutivo para desarrollar el artículo 18.4 de la Constitución Española, referente al uso de la informática. Si bien es cierto que esta iniciativa gubernamental no es producto de una sentencia como en el caso portugués, sí lo es de una serie de eventos. Entre ellos cabe destacar el Convenio de Estrasburgo firmado en Septiembre de 1980 y ratificado por el Estado Español en 1984. Dicho Convenio se publicó en el B.O.E. de 15 de Noviembre de 1985.

CONSTITUCIONES IBERICAS

La Península Ibérica nos ha aportado la primicía de un derecho fundamental de Protección de Datos, a saber, en el artículo 35 de la Constitución Portuguesa de 1976 y en el artículo 18 de la Constitución Española de 1978. Resulta significativo que estas dos Constituciones, las más modernas de Europa, tengan ambas un derecho especial de protección de datos, como norma pre-legislativa.

La primera analogía, pues, con la que nos encontramos entre los dos países Ibéricos, relativa al tema que nos ocupa, es el Tratamiento Informático en sus respectivas Leyes Supremas; ya que, tanto en España como en Portugal, la protección del ciudadano contra los daños causados por el ordenador, figura en ambas Constituciones.

Como apuntábamos antes, este dato no es un hecho generalizado en todos los países; es decir, que en la Ley Suprema de un Estado se haga referencia a la informática y a la protección de las libertades individuales. Es por ello, que esta primera analogía apuntada se torne tan significativa.

Sin embargo, a esta analogía, debemos añadir inmediatamente sus diferencias. Esto es, su distinta redacción en ambas Constituciones.

Se suele considerar, en esta materia, que nuestra Constitución se ha inspirado en la portuguesa de 1976, cuyo artículo 35 (ubicado en el Título II «de los derechos, libertades y garantías») está dedicado a la «utilización de la Informática». Ahora bien, conviene indicar, evitando posibles equívocos, que el texto portugués es mucho más detallado que el correspondiente de Constitución Española.

Así pues, el texto íntegro del artículo 35 de la Constitución de la República Portuguesa, de 1976, reza así:

«1.–Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.

2.–La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.

3.–Queda prohibida la atribución de un número nacional único a los ciudadanos.»

De otro lado, la Constitución Española de 1978 no se pronuncia claramente acerca de si ha de primar el valor individual de la intimidad o el interés social de la información; pues, parece eludir el tema, tratando de quedarse con el más cómodo punto de equivalencia, según el cual tanto monta para el Estado un valor como el otro.

La citada Constitución española aborda la materia, en cuanto a la información general, en su artículo 20.1; mientras que el artículo 105, b), con carácter programático y empleando para ello el tiempo futuro, dice que la Ley regulará el libre acceso de los ciudadanos a los archivos y registros.

Con literal mención a la informática, el artículo 18.4 de la referida Constitución determina, también con carácter programático, que :«La Ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Uno de los problemas que plantea el artículo 18 en su apartado 4, no consiste en saber si los derechos cuyo pleno ejercicio garantiza pertenecen o no al ámbito de la protección de la esfera privada, sino en individualizar cuáles son los derechos que, aun perteneciendo a ese ámbito, van más allá del «honor y la intimidad personal y familiar».

En este sentido, merece destacarse que la Constitución de la República Portuguesa sigue la tendencia general de englobar los datos relativos a la vida privada entre las categorías de datos que reciben una disciplina especial dentro del régimen general aplicable a los datos personales. Es por ello, que el texto del artículo 35 de la Constitución Portuguesa es mucho más detallado que el artículo 18.4 de la Constitución Española.

«DECADA DE LOS 90»

Pero ambos preceptos Constitucionales Ibéricos, necesitan un posterior desarrollo legislativo. Nos topamos pues, con otra analogía Ibérica: La «Década de los 90»; ya que no es hasta esta fecha cuando se redactan las Leyes de Protección de Datos. Si bien es cierto, que mientras la Ley Portuguesa fue publicada en el Diario de la República el 29 de Abril de 1991, la correspondiente Española está aún en el Congreso; pues, en España no podemos hablar aún de Ley, sino de Proyecto de Ley (LORTAD español). El citado proyecto, fue aprobado por el Consejo de Ministros el pasado 28 de Junio de 1991, para remitirlo al Congreso, cuyo Boletín Oficial de las Cortes Generales lo recoge, como proyecto de Ley, en el de fecha 24 de Julio de 1991.

El nacimiento de una y otra Ley procede de una característica común: un «Mandato Constitucional», y a su vez, de elementos distintos para una y otra.

Así en el caso Portugués, la Lei núm. 10/91 «Lei da PROTECÇAO de Dados Pessoais face Informática» nace como consecuencia de la Sentencia del Tribunal Constitucional Portugués «ACORDAO n.º 182/89-PROCESSO n.º 298/87».

En esta sentencia, se pone de manifiesto el no cumplimiento de la Constitución, por la omisión de una medida legislativa para dar cumplimiento al artículo 35 de dicha Ley Suprema. Así mismo, se da conocimiento, de ello, a la Asamblea de la República. A causa pues, de esta Sentencia, el Gobierno Portugués se ve en la obligación de dictar una Ley de Protección de Datos. Esta última, se publicaría en el Diario de la República en su n.º 98 el 29 de abril de 1991. Más adelante, volveremos a la citada ley.

Hablemos ahora, de las posibles causas que han dado nacimiento al Proyecto de LORTAD español; pues, aunque también obedece a un mandato constitucional (como la ley portuguesa), no así, a una sentencia.

El análisis del apartado 4 del artículo 18 de la Constitución española lleva a diversas interpretaciones; ya que, no parece del todo satisfactoria la redacción del texto constitucional en lo que afecta a los derechos que estamos contemplando. Es por ello, que el posterior desarrollo de estos preceptos, se estaba haciendo esperar demasiado. Pues el constituyente ha previsto que, sin una regulación legal, existen riesgos graves para los derechos fundamentales de la persona por el uso incontrolado y sin las debidas garantías de la informática. El constituyente, efectivamente, no dice que no se deba utilizar la informática, sino que su uso debe estar acompañado de unas debidas garantías. De otro lado, en Septiembre de 1980 se firma en Estrasburgo una «Convención para la protección de las personas frente al tratamiento automático de los datos de carácter personal». Se trata del primer texto internacional adoptado en este terreno. En 1984, el Estado español ratifica el citado convenio, que publicó en el B.O.E. de 15-11-1985, y que, de acuerdo con la Constitución española (art. 96) dicho convenio, queda incorporado al ordenamiento jurídico español en virtud de su publicación oficial en España.

Sin embargo, una nueva lectura al texto de Estrasburgo, nos percata de que éste, por sí mismo, es insuficiente; pues, hay una referencia a las legislaciones internas de los Estados de la Convención. Por ello, el Convenio no puede constituir el desarrollo del artículo 18.4 de la Constitución; puesto que, se trata de una normativa marco de principios que remite reiteradamente a las medidas legislativas de derecho interno. Además, el artículo 12 del Convenio condiciona la transmisión de datos personales informatizados al desarrollo de garantías de tutela del mismo; por lo que, puede ser denegada esa transmisión de información, por parte de cualquier Estado firmante del Convenio, si se comprueba la ausencia de medidas legislativas al respecto.

Pero, no ha sido el Convenio la única causa (después del mandato constitucional), del nacimiento del Proyecto de LORTAD español.

En los últimos tiempos se ha verificado en España una incontrolada informatización de datos, tanto en el sector público como en el privado. Los ciudadanos, desconocen los datos que sobre su persona se han informatizado, con qué finalidad, y cuáles son las interconexiones a las que han sido sometidos.

El Ordenamiento Jurídico Español contiene respuestas fragmentarias y marginales para la tutela de la libertad informática de las personas. La propia Constitución de este país, como apuntábamos antes, no se pronuncia claramente, acerca de si ha de primar el valor individual de la intimidad o el interés social de la información.

El 5 de Mayo de 1982, se aprueba la Ley Orgánica de Protección Civil del «Derecho al Honor, a la Intimidad personal y familiar y a la propia Imagen». La finalidad de esta Ley, según reza en ella, es el desarrollo del

principio general de garantía de tales derechos contenidos en el artículo 18.1. de la Constitución Española.

Esta ley, no se refiere a la protección de tales derechos frente a la informática; pero, en su Disposición Transitoria Primera, establece que «en tanto no se promulgue la normativa prevista en el artículo 18, apartado 4, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática, se regulará por la presente Ley». Sin embargo, el alcance de esta declaración es prácticamente nulo; puesto que, la propia Ley, no establece cuáles son esas intromisiones ilegítimas a las que se refiere. No obstante, es el texto en vigor, sobre el tema que nos ocupa, hasta que el Proyecto de LORTAD español no se traduzca en Ley. Ello se desprende, no sólo de lo dicho, sino también de la Disposición Derogatoria del Proyecto de LORTAD español (en la que se deroga la disposición transitoria primera de la Ley Orgánica 1/1982 de 5 de Mayo).

Existen en España ciudadanos preocupados por el uso de la informática; los cuales, han acudido a la institución del Defensor del Pueblo. Ello, revela que la situación de laguna legal sobre el uso de datos debe de terminar cuanto antes.

En el Ordenamiento Jurídico Español, pueden encontrarse disposiciones aisladas pero no suficientes (con respecto al tema). Este hecho ha llevado a recoger en el informe anual del Defensor del Pueblo (hecho público el 15 de abril de 1991), la necesidad de que se articule una Ley, que regule el uso de la informática por parte de la Administración, que limite la toma de datos cuando se refieren al ámbito reservado de la intimidad de la persona.

Todo lo anterior, ha llevado a que el Gobierno Español haya ultimado su proyecto de Ley Orgánica para la Regulación del Tratamiento Automatizado de Datos de Carácter Personal.

Este Proyecto de Ley, fue elaborado por el Ejecutivo para desarrollar el artículo 18.4 de la Constitución Española, referente al uso de la informática; y, supone la modificación de la actual legislación sobre protección de datos informáticos en dos aspectos principales: el acceso de los interesados a los datos y las garantías sobre rectificación y uso de los mismos.

Recordemos que el citado Proyecto (como dijimos más arriba), fue aprobado por el Consejo de Ministros el pasado 28 de Junio de 1991, para remitirlo al Congreso, cuyo Boletín Oficial de las Cortes Generales lo recoge, como proyecto de ley, en el de fecha 24 de Julio de 1991. En el momento de escribir estas líneas, el citado texto permanece aún en el Congreso, para su estudio. Se espera que, en breve se torne realidad ese proyecto de Ley.

ESTRUCTURACION DE AMBAS LEYES

Aunque a lo largo del articulado, encontremos semejanza entre ellos, por los temas a tratar, en un esquema general ya, encontramos diferencia; pues, la Ley Portuguesa dividida sólo en Capítulos va especificando en cada artículo de qué trata el mismo. Esto, no ocurre en el Proyecto LORTAD español. Este último, sin embargo, posee una «EXPOSICION DE MOTIVOS» inexistente en la Ley Portuguesa, en la que se explica el contenido y su por qué a juicio del legislador.

El Proyecto español se nuclea en torno a los que convencionalmente se denominan «Ficheros de datos». Animada por la idea de implantar mecanismos cautelares, que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información, la futura ley española se estructura, a tal efecto, en una Parte General y otra Especial.

La PARTE GENERAL comprende los tres primeros títulos:

– «Título Primero» dedicado a las «Disposiciones Generales», comprende los artículo 1, 2 y 3.

– «Título Segundo»: trata de «Principios de la Protección de Datos», artículos 4 al 11.

– «Título Tercero»: «Derechos de la Persona», artículos 12 al 17.

La PARTE ESPECIAL comienza en el «Título Cuarto» de la Ley, abarcando también los Títulos Quinto, Sexto y Séptimo.

El «Título Cuarto», cuyo nombre reza «Disposiciones Sectoriales» se divide en dos capítulos. A saber «Capítulo Primero: Ficheros de titularidad Pública» (arts. 18 al 22) y «Capítulo Segundo: Ficheros de titularida Privada» (arts. 23 al 31).

ANTONIO E. PÉREZ LUÑO Doctor en Derecho por la Universidad de Bolonia. Consejero científico de Informática e Diritto (Florencia). Miembro del Consejo ejecutivo del Centro de Análisis, Lógica e Informática Jurídica y del Instituto de Derechos Humanos de la Universidad Complutense de Madrid.

El Título Quinto de «Movimiento Internacional de Datos» comprende los artículos 32 y 33.

El Título Sexto está dedicado a la «Agencia de Protección de Datos», artículos 34 al 41.

El Título Séptimo es «Infracciones y Sanciones» (arts. 42 al 48).

Este Proyecto de Ley se completa con tres Disposiciones ADICIONALES, una DEROGATORIA, cinco Disposiciones FINALES y una Disposición TRANSITORIA.

Hagamos ahora, un esquema general de la Ley Portuguesa para poder, más tarde, equipararlas mejor.

LEI N.º 10/91 «LEI DA PROTECÇAO DE DADOS PESSOAIS FACE E INFORMATICA»:

CAPITULO I, lleva por título DISPOSICIONES GENERALES y comprende los siguientes artículos:

-artículo 1: Principio General
-artículo 2: Definiciones
-artículo 3: Ambito de Aplicación.

Como apuntábamos antes, en esta ley, no sólo llevan un nombre los capítulos sino también cada artículo.

CAPITULO II, «De la Comisión Nacional de Protección de datos Personales Informatizados» (en adelante en la ley se alude a este organismo con las siglas C.N.P.D.P.I.). Este capítulo comprende los artículos siguientes:

-artículo 4: Creación y Atribuciones
-artículo 5: Composición
-artículo 6: Deberes e Incompatibilidades
-artículo 7: Estatuto Remunerativo
-artículo 8: Competencias
-artículo 9: Deber de Colaboración
-artículo 10: Posesión (del cargo de C.N.P.S.P.I.)

CAPITULO III, «Del Proceso de Datos Automatizados de Datos Personales».

-artículo 11: Restricciones al Tratamiento de datos
-artículo 12: Requisitos de Recogida
-artículo 13: Derecho de Información y Acceso
-artículo 14: Actualización de datos
-artículo 15: Utilización de Datos
-artículo 16: Límites de la Apreciación Judicial

CAPITULO IV, «De los Ficheros Automatizados, de Bases y de Bancos de Datos Personales».

-artículo 17: Requisitos de Constitución
-artículo 18: Instrucciones de los Pedidos (para pedir los ficheros)
-artículo 19: Indicaciones Obligatorias
-artículo 20: Funcionamiento de los Ficheros
-artículo 21: Equipamiento de Seguridad

CAPITULO V, «De la Recogida y de la Interconexión de Datos Personales».

-artículo 22: Indicaciones constantes de datos personales
-artículo 23: Destrucción de datos
-artículo 24: Interconexión de datos públicos
-artículo 26. Casos Excepcionales

CAPITULO VI, «De los Derechos y Garantías Individuales».

-artículo 27: Derecho de acceso a las informaciones

-artículo 28: Ejercicio del derecho de acceso
-artículo 29: Exceso u Omisión de Datos
-artículo 30: Informaciones inexactas
-artículo 31: Intervención del Responsable (del soporte informático)
-artículo 32: Secreto Profesional

CAPITULO VII. «Flujo de Datos Transfronterizo».
-artículo 33: Régimen aplicable

CAPITULO VIII, «Infracciones y Sanciones».
-artículo 34: Utilización ilegal de datos
-artículo 35: Obstrucción al acceso
-artículo 36: Interconexión ilegal
-artículo 37: Falsas informaciones
-artículo 38: Acceso indebido
-artículo 39: Vicios o destrucción de datos
-artículo 40: Desobediencia cualificada
-artículo 41: Violación del deber de secreto
-artículo 42: Punición de Tentativa
–artículo 43: Pena accesoria

CAPITULO IX, «Disposiciones Transitorias y Finales».
-artículo 44: Reglamentación
-artículo 45: Legalización de los soportes existentes.

Retomando nuevamente el Proyecto de Ley Español, y haciendo una breve comparación con la Ley Portuguesa, lo primero que vemos es que, los tres primeros artículo de ambas leyes, poseen notables similitudes. Así el CAPITULO I de la ley portuguesa vendría a ser el Título Primero de la española, en ambas se refieren a «Disposiciones Generales».

En el artículo 1 del Proyecto Español encontramos el «objetivo» de dicha ley: «el cumplimiento de una normativa Constitucional (el artículo 18.4 de la C.E.)». Esta ley pretende «limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos».

A su vez, en el artículo 1.º de la Ley portuguesa, vemos su principio general; el cual reza así: «El uso de la informática debe procesarse de forma transparente y en el estricto respeto por la reserva de la vida privada y familiar y por los derechos, libertades y garantías fundamentales del ciudadano».

En realidad, aunque expresada en distinta redacción, la intención de ambos legisladores viene a ser la misma.

El artículo 2.º de la Ley Portuguesa se dedica a las «Definiciones» a efecto de esa ley. Lo mismo hace el artículo 3 del Proyecto español; si bien es más amplio el artículo portugués. A saber, en este último se definen los conceptos siguientes: «Datos Personales», «Datos Públicos», «Sistema Infor-

mático», «Fichero Automatizado», «Base de Datos», «Banco de Datos», «Tratamiento Automatizado», «Responsables de los soportes informáticos» y «Flujo de datos transfronterizo».

El artículo 3 del Proyecto LORTAD español acoge las siguientes definiciones: «Datos de carácter personal», «Fichero Automatizado», «Tratamiento de datos», «Responsable del fichero», y «Afectado» (ésta última no aparece en la ley portuguesa).

Puede apreciarse, que de todas las definiciones, sólo cuatro coinciden en ambas leyes.

El artículo 3.º de la Ley Portuguesa se correspondería con el artículo 2 del Proyecto español; pues ambos tratan el «Ambito de Aplicación» de cada ley.

Si nos fijamos, en la Parte General del Proyecto español, nos percatamos que en ella se recogen los Principios Generales, así como, que se definen derechos y garantías aseguradoras de tales principios.

Se compone, pues, esta Parte General, además de los preceptos delimitadores del ámbito de aplicación de la ley, los Principios Reguladores de la Recogida, Registro y Uso de datos personales, y sobre todo, Garantías de la persona. Estas últimas, son las nutrientes nucleares de dicha Parte General, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Estas garantías, traducidas en derechos, nos las encontramos tanto en el Título Segundo cono en el Título Tercero. A su vez, estos dos títulos vendrían a equipararse a 3 CAPITULOS de la Ley Portuguesa; a saber CAPITULO III, CAPITULO V y CAPITULO VI.

Los Principios Reguladores, los encontramos en ambas leyes y básicamente serían: Principio de Veracidad, Principio de Congruencia y Racionalidad, Principio del consentimiento o Autodeterminación.

Como correlato de los Principios, se plasman en ambos textos, Los Derechos de Autodeterminación (derecho a ser informado), de Acceso a los datos, de Rectificación y de Cancelación.

Básicamente, podría decirse que el CAPITULO VI («De los Derechos y Garantías individuales») de la ley portuguesa se corresponde con el TITULO III («Derechos de las Personas») de la ley española; con la salvedad, que el «Secreto Profesional» recogido en el artículo 32 de dicho Capítulo VI (de la ley portuguesa), encuentre su homólogo «Obligación de guardar silencio» (del responsable y de las personas que intervengan en cualquier fase del Tratamiento) en el artículo 10 de la ley española, cuya ubicación es el TITULO II de dicha ley. No obstante, a lo largo de ambas leyes, podemos encontrarnos con los Principios informadores de las mismas y sus correlatos derechos y deberes (como Garantías de las Personas).

Centrándonos ahora en la Parte Especial del Proyecto LORTAD español, nos topamos con el TITULO IV donde comienza dicha parte. En él la ley establece regímenes diferenciados para los ficheros en razón de su titularidad. Así, el Capítulo Primero de dicho Título está dedicado a los «Ficheros de titularidad pública» y el Capítulo Segundo del mismo Título, lo está a los «Ficheros de titularidad privada». Distinción, esta última, que no realiza la ley portuguesa en su parte homóloga; la cual, sería el CAPITULO IV dedicado a «Ficheros automatizados, bases y bancos de datos personales».

La Transmisión Internacional de los datos son otras disposiciones que aparecen recogidas en ambas leyes. A saber, en el TITULO QUINTO de la ley española dedicado al «Movimiento Internacional de Datos», y en el CAPITULO VII de la ley portuguesa, que lleva por nombre «Flujos de Datos Transfronterizos».

Ambas leyes, con el fín de asegurar la máxima eficacia de sus disposiciones, encomienda el control de su aplicación a un órgano independiente y especializado. En la ley portuguesa se trata de la C.N.P.D.P.I. (Comisión Nacional de Protección de Datos Personales Informatizados); a la que dedica su CAPITULO II.

En la ley española, el órgano aludido, se denomina «Agencia de Protección de Datos», recogida en el TITULO VI de dicho Proyecto LORTAD español.

Si bien, la función, de ambos órganos, pretende ser la misma, lo cierto es que no son, en rigor, totalmente idénticos.

La «Agencia de Protección de Datos», a cuyo frente se sitúa un Director (esta figura no aparece en la C.N.P.D.P.I. portuguesa), es un Ente de Derecho Público (según reza el artículo 34), con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas (en el ejercicio de sus funciones).

Según el artículo 4.1 de la ley portuguesa, la C.N.P.D.P.I es también una entidad pública independiente con poderes de autoridad, pero que funciona junto a la Asamblea de la República y dispone de servicios propios de apoyo técnico y administrativo.

Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos española, serán desempeñados por funcionarios de las Administraciones Públicas y por personal contratado al efecto. A su vez, dicha Agencia dispondrá de un órgano de apoyo, definido por los caracteres de colegiación y representatividad. Es el Consejo Consultivo, (el cual no existe en la C.N.P.D.P.I. portuguesa).

La composición de la C.N.P.D.P.I. es de siete miembros; el Presidente y 2 vocales son elegidos por la Asamblea de la República, y los restantes vocales son 2 Magistrados y 2 personalidades designados por el Gobierno. Su posesión en el cargo es por un período de 5 años.

Sin embargo, la ley española, con el fin de garantizar la absoluta independencia del Director de la Agencia, en el ejercicio de sus funciones, (lo cual es un expreso imperativo legal) no sólo establece un mandato fijo (período de 4 años, especifica el art. 35), sino que éste sólo puede ser acortado por «numerus clausus» de causas de cese. Estas pueden ser de dos tipos: a) a petición propia, o b) por separación acordada por el Gobierno, (previa instrucción del expediente); las causas de separación son: por incumplimiento grave de sus obligaciones; incapacidad sobrevenida para el ejercicio de sus funciones; incompatibilidad; condena por delito doloso.

En la ley portuguesa no aparecen ninguna de estas causas de cese; por lo que, se entiende que los miembros de la Comisión sólo cesarán cuando acabe su mandato (5 años).

La última parte de ambas leyes, «TITULO SEPTIMO» del proyecto LORTAD español y «CAPITULO VIII» de la ley portuguesa versa sobre lo mismo: «INFRACCIONES Y SANCIONES». Si bien, también aquí, encontramos diferencias.

En la ley española, aunque fuera de ese Título VII, recoge normas de autorregulación compatibles con las recomendaciones de la Agencia (tales como: la creación de Códigos tipo, que tienen la consideración de códigos deontológicos), se le da también capacidad de inspección a la Agencia y capacidad de impugnación al Director de la misma; no obstante, en su Título VII, el Proyecto LORTAD no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento.

Lo que sí hace esta ley es atribuir a la Administración la potestad sancionadora, similar a las demás inspecciones administrativas. Esta potestad se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, o sobre los privados. En el primer caso (los públicos) procederá la oportuna responsabilidad disciplinaria; para los privados se prevén sanciones pecuniarias.

Por otro lado, la ley se limita a tipificar unos supuestos genéricos de responsabilidad administrativa, recogiendo una gradación de infracciones (que sigue la habitual distinción) entre Leves, Graves y Muy Graves (art. 43) y que toma como criterio básico el de los bienes jurídicos emanados.

No obstante, aparte de las Sanciones pecuniarias y responsabilidad disciplinaria antes aludida, la ley articula la posibilidad de «inmovilizar los ficheros» (art. 48) en los supuestos: constitutivos de infracción muy grave; de cesión ilícita de datos; o de cualquier otro atentado contra los derechos de los afectados que revistan gravedad.

También se recogen en esta ley (art. 46) las Prescripciones tanto de las infracciones como de las sanciones. El procedimiento a seguir para determinar tales infracciones y la imposición de sanciones, se hará por vía Reglamen-

taria (art. 47.1). Contra las resoluciones de la Agencia (art. 47.2), procederá recurso contencioso-administrativo.

Por el contrario en la Ley Portuguesa, cada artículo de ese Capítulo VIII, especifica un delito; y el Procedimiento a seguir, no será administrativo sino criminal; el Procedimiento criminal a seguir dependerá de la «queixa» (causa).

En la ley portuguesa no aparecen las Prescripciones de los delitos y penas articulados en la misma.

Una gran novedad, con respecto a la ley española es la imposición de la pena de Prisión (el proyecto español, como dijimos, no pasa de establecer multas pecuniarias). Así, en los artículos 34 («utilización ilegal de datos»), 35 («obstrucción al acceso»), 36 (interconexión ilegal»), y 38 («acceso indebido»), la pena registrada es prisión hasta 1 año o multa de hasta 120 días. Esta pena, a su vez, puede ser agravada en determinados casos. Así mismo, también se pena al agente que actúa con negligencia (art. 35), prisión de hasta 3 meses o multa de hasta 90 días.

En los artículos 37 («Falsas informaciones»), 39 («Vicios o destrucción de datos») y 40 («Violación del deber de secreto»), la pena de Prisión es hasta 2 años o multa hasta 240 días. Aunque esta pena también puede ser agravada, dependiendo de particularidades, la misma es menor en el caso de que sea el Agente el que actúa con negligencia. A saber, Prisión de 1 año o multa de hasta 120 días en caso de «Violación del deber de secreto» (art. 41); y prisión de hasta 6 meses o multa hasta 100 días en el caso del art. 37 (Falsas informaciones»).

A estas penas principales, el Tribunal puede ordenar la Pena Accesoria (art. 43) de publicidad de la sentencia condenatoria, íntegra o por extracto, a expensas del condenado, en una o más publicaciones periódicas.

No existen penas accesorias en la ley española, pues como dijimos, dicha ley sólo se limita a imponer multas pecuniarias, no consagrando tipos delictivos. Por esta última razón, tampoco en el proyecto español, se registra el grado de tentativa, pues esta ley sólo se limita a clasificar las infracciones en leves, graves y muy graves. Sin embargo, en la ley portuguesa el grado de TENTATIVA de los delitos registrados en los artículos 34 al 41, es siempre punible, así reza el artículo 42.

Las multas a las que nos hemos referido en el proyecto LORTAD español son: de 100.000 a 10.000.000 de pesetas para infracciones leves; de 10.100.000 a 50.000.000 de pesetas para infracciones graves; y de 50.100.000 a 100.000.000 millones de pesetas para infracciones muy graves. La cuantía de éstas sanciones (según la ley, art. 44), se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia.

Queda patente pues, la notable diferencia en ambas leyes al tratar esta sección de «Infracciones y Sanciones».

De las últimas disposiciones, cabe citar la que es Transitoria en ambos textos legales. Esta se justifica por la necesidad de ajustar la utilización de los ficheros existentes a las disposiciones legales.

CONCLUSION

A lo largo de estas breves reflexiones, nos percatamos del interés de ambos países ibéricos por el tema que nos ocupa: «LA PROTECCION DE DATOS». Esta preocupación se ha visto traducida en textos legales de ambos países, que aunque con distinta factura, pueden considerarse homólogos.

La LORTAD: breve análisis de sus antecedentes

JOSÉ JAVIER SANTAMARÍA IBEAS
Licenciado en Derecho. Profesor Ayte. de Filosofía del Derecho en la Universidad de Valladolid
(ESPAÑA)

SUMARIO

1. INTRODUCCION
2. ANTECEDENTES DE LA LORTAD:
   2.1. Regulación constitucional.
   2.2. Jurisprudencia del TC.
   2.3. Convenios Internacionales.
   2.4. Proyectos legislativos españoles.
3. CONCLUSIONES

1. INTRODUCCION

El contenido de la presente comunicación se refiere al Proyecto de Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), que se halla esperando la aprobación de su texto definitivo por parte del legislador español[1]. La comunicación se redactó en agosto de 1992, y ello quiere decir que si el texto definitivo de la LORTAD apare-

[1] El Proyecto fue remitido a las Cortes por el Gobierno y está publicado en el Boletín Oficial de las Cortes Generales, Congreso de los Diputados, Serie A, n.º 59-1, de 24 de julio 1991. Fue aprobado por el Pleno del Congreso el día 20 de marzo de 1992 y entró en el Senado del día 25 del mismo mes.

ciera en septiembre, al regreso de las vacaciones estivales [2], lo que en este trabajo se refiere al texto positivo de la LORTAD se habría de entender modificado, ya que, aunque no es previsible que el Proyecto sufra numerosas alteraciones en su paso por las Cámaras legislativas, dichas alteraciones pudieran resultar cualitativamente importantes, a la vista de las posiciones que han tomado y de las enmiendas que tratan de introducir determinadas organizaciones sociales en el texto definitivo de la LORTAD [3].

2. ANTECEDENTES DE LA «LORTAD»

2.1. Regulación constitucional.

La Constitución Española de 1978 (CE a partir de ahora), debido a la fecha en que se produce su elaboración, prevé de forma explícita lo que ya en la década de los años '70 comenzaba a ser evidente: la creciente utilización de la Informática para la gestión de los datos personales de los ciudadanos.

Así, la CE contiene dos preceptos básicos en el Capítulo II, Sección 1.ª («De los derechos fundamentales y de las libertades públicas»): por una parte, como salvaguardia general de estos derechos fundamentales, establece el apartado 2.º del artículo 16:

> «Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.»

Y, refiriéndose en concreto a la garantía del derecho a la intimidad personal, establece en el apartado 4.º del artículo 18:

> «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.»

A la vista de este artículo 18.4 CE es obvia –y creo que criticable– la aparente predisposición negativa del constituyente español respecto de la utilización de la Informática, desde el momento en que, con la perspectiva que tiene en 1978, no habla de «regular», sino de «limitar»; más aún si tenemos en cuenta que este art. 18.4. es uno de los preceptos básicos en los que se ha de fundamentar la promulgación de una ley reguladora de la gestión de los datos personales.

---

[2] Aunque también pudiera suceder que el Gobierno no agotase su mandato, convocando la celebración de Elecciones Generales anticipadas, de modo que habrían de disolverse las Cámaras y quedaría el Proyecto sin tramitar, al menos en la presente legislatura.

[3] Podríamos señalar incluso, un cierto paralelismo entre las desgarradas críticas que se vertieron en contra de la redacción definitiva de la Ley Orgánica de Protección de la Seguridad Ciudadana y las que ha recibido el Proyecto de LORTAD, en concreto sus artículos 19-22, por parte de organizaciones tales como la *Comisión de Libertades Informáticas,* que ha anunciado su intención de recurrir la LORTAD en el caso de que los debates que se celebren en el Congreso y en el Senado no modifiquen sustancialmente ciertos preceptos en la redacción definitiva (tal declaración de intenciones se recoge en el periódico «Diario 16» del viernes 8 de mayo de 1992). (La CLI está integrada por asociaciones tales como la Asociación de Técnicos en Informática, Asociación Pro Derechos Humanos, Unión General de Trabajadores, etc.)

Además de los señalados artículos, igualmente habrán de ser tenidos en cuenta otros preceptos no incluidos dentro de la Secc. 1.ª del Cap. 2.º –derechos fundamentales y libertades públicas–. Así, el art. 81 CE., que establece la necesidad de que determinadas materias –como los derechos fundamentales– sean reguladas a través de Leyes orgánicas [4]; y el art. 105, en el que se establece que la ley regule el denominado «derecho de acceso», es decir, la posibilidad que deben tener todos los ciudadanos de conocer los datos personales a ellos referidos que se contengan en los archivos de la Administración [5].

2.2. Jurisprudencia del Tribunal Constitucional.

Resulta conveniente señalar que el objetivo que han de pretender las normas de cualquier ordenamiento dirigidas a regular la utilización y manipulación de los datos personales, no es la protección en abstracto de esos datos, sino proteger y asegurar los derechos propios de la persona a la que se refieren los datos. Ello resulta obvio si analizamos cualquiera de las definiciones de «datos personales» que aparecen en distintos textos de Derecho comparado [6].

Desde este punto de vista de protección de los derechos de la persona a la que se refieren los datos, es desde el que podemos entender la posibilidad que otorga el art. 53.2. CE de acudir al TC a través del recurso de amparo, en el caso de que se produzca una transgresión del derecho a la intimidad.

Dentro del art. 18 CE, ya señalamos que es el apartado 4.º el que hace una referencia expresa a la utilización de la Informática pero, dado que este apartado remite a un desarrollo legislativo posterior («la ley limitará...»), el TC no ha tenido oportunidad de conocer ningún recurso presentado con base en este apartado concreto, aunque sí en los tres restantes. De esta forma, las sentencias del TC a que aludiremos a continuación no se refieren al art. 18.4, pero son útiles porque delimitan un concepto fundamental para la regulación

---

[4] Art. 81.1: «Son leyes ***orgánicas*** las relativas al desarrollo de los ***derechos fundamentales*** y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.»

[5] Art. 105: «La Ley regulará: b) El ***acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.***»

[6] El Convenio n.º 108 del Consejo de Europa del año 1981, al que más adelante nos referimos, expresa en su art. 2 bajo la rúbrica de «Definiciones»: «Datos de carácter personal siginifica cualquier información relativa a una persona física identificada o identificable (persona concernida).»

Igualmente, la Loi relative `a l'informatique, aux fichiers et aux libertés (Francia 1978), define a los «Datos personales» en su art. 4.º: » ... les informations qui permettent, sous quelque forme que ce soit, directement ou non l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale.»

de la protección de datos personales: el concepto de intimidad, aunque sea aprovechando el análisis que se hace de los otros apartados del art. 18 CE:

a) STC 110/1984, de 26 de noviembre: Esta no es la primera STC que se refiere al art. 18 CE, pero es la primera que recogemos porque concreta el derecho a la intimidad referido a los datos personales al conocer un recurso de amparo interpuesto por una persona física que suplica al TC que anule una disposición de la Administración del Estado que autoriza la investigación de sus operaciones activas y pasivas en determinadas entidades bancarias, pretendiendo el recurrente que el TC declarase que dichos datos se refieren a su intimidad económica y, por lo tanto, forman parte de su *«intimidad constitucionalmente protegida»* (por el art. 18 CE). El TC, al conocer el recurso de amparo –denegado–, caracteriza el derecho a la intimidad:

> «(...) La inviolabilidad de domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y del desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito de reservado de la vida. (...) «(Fundamento jurídico 3.º).».
>
> «(...) Todo derecho tiene sus límites que en relación a los derechos fundamentales establece la Constitución por sí misma en algunas ocasiones, mientras en otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionales protegidos.(...)» (Fundamento jurídico 5.º).

Vemos como el TC fundamenta la denegación del recurso de amparo –y, por lo tanto, la declaración de la licitud de la investigación llevada a cabo por la Administración sobre las cuentas bancarias del recurrente– en dos principios básicos de la jurisprudencia constitucional: a) los límites a los que están sometidos todos los derechos fundamentales recogidos en la CE [7] y, b) el conflicto entre derechos o entre bienes constitucionalmente protegidos [8].

b) STC 53/1985, de 11 de abril [9]. El Tribunal, al conocer del recurso de inconstitucionalidad planteado, hace una nueva caracterización del conte-

[7] En este caso, la intimidad estaría limitada «por el deber de todos de contribuir al sostenimiento de las cargas públicas de acuerdo con su capacidad económica.» (Fund. jco. 8.º).

[8] Aquí chocarían el derecho fundamental a la intimidad y, «el bien constitucionalmente protegido que es la distribución equitativa del sostenimiento de los gastos públicos» (Fund. jco. 5.º).

[9] Esta STC responde al recurso previo de inconstitucionalidad (2 diciembre 1983) que

nido de los derechos fundamentales, de sus límites y, además, se refiere de modo expreso al mandato contenido en el art. 18.4:

> «(...) la doctrina ha puesto de manifiesto –en coherencia con los contenidos y estructuras de los ordenamientos positivos– que los derechos fundamentales no incluyen solamente derechos subjetivos de defensa de los individuos frente al Estado, y garantías institucionales, sino también deberes positivos por parte de éste (vide al respecto arts. 9.2, 17.4, 18.1 y 4, 20.3 y 27 de la Constitución). (...)
>
> (...) Por consiguiente, de la obligación del sometimiento de todos los poderes a la Constitución, no solamente se deduce la obligación negativa del Estado de no lesionar la esfera individual o institucional protegida por los derechos fundamentales, sino también la obligación positiva de contribuir a la efectividad de tales derechos, y de los valores que representan, aun cuando no exista una pretensión subjetiva por parte del ciudadano. Ello obliga especialmente al legislador, quien recibe de los derechos fundamentales 'los impulsos y líneas directivas', obligación que adquiere especial relevancia allí donde un derecho o valor fundamental quedaría vacío de no establecerse los supuestos para su defensa. (...)» (Fundamento jurídico 4.º).

Posiblemente, en esta STC es en la que mejor podemos observar como la jurisprudencia del TC recoge el mandato constitucional del art. 18.4. CE. El TC, acorde con el constitucionalismo actual inspirado en el Estado social de Derecho, declara que el respeto a los derechos fundamentales de la persona (en concreto, el derecho a la intimidad) no puede ser llevado a cabo por parte del Estado manteniendo una actitud pasiva o simplemente negativa, de no vulneración, sino que el Estado ha de desarrollar positivamente esos derechos, más aún cuando –como textualmente señala la STC– hay un mandato legal expreso, (el contenido en el art. 18.4. CE) [10].

c) STC 171/1990, de 5 de noviembre [11]: Analiza la colisión que se puede producir entre el derecho a la intimidad y el de libertad de información, dejando claro que ésta prima sobre aquél, aunque reconoce ciertas limitaciones derivadas del interés público que tenga o no tenga dicha información:

> «Dada su función institucional, cuando se produzca una colisión de libertad de información con el derecho a la intimidad y al honor aquella goza, en general, de una posición preferente y las restricciones que de dicho conflicto pueden

---

interpuso el Grupo Popular del Congreso de los Diputados contra el «Proyecto de Ley Orgánica de Reforma del artículo 417 bis del Código Penal», es decir, en contra de la reforma del Cp. despenalizadora de determinados supuestos de aborto.

[10] De esta forma, el Estado adquiere para con sus ciudadanos un auténtico deber jurídico, semejante a una obligación de hacer –en este caso de legislar–, para fomentar el respeto de los derechos de la persona (y el art. 18.4 CE sería un claro ejemplo de este tipo de deber).

[11] Esta STC se dictó para resolver un recurso de amparo –estimado– interpuesto ante el TC por el director «El País», al considerar vulnerado el art. 20 de la CE –libertad de información– por la Sentencia del TS (Sala Primera) de 7 marzo 1988 –en casación– que condenaba a los diarios «El País» y «Diario 16» a publicar dicha Sentencia en primera página y a pagar, por la publicación de determinada información referida al piloto de un avión de pasajeros siniestrado en las cercanías del aeropuerto de Bilbao en 1985, una indemnización a sus herederos.

derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional desnaturalizado ni incorrectamente relativizado. (...)

Tal valor preferente, sin embargo, no puede configurarse como absoluto, puesto que, si viene reconocido como garantía de la opinión pública, solamente puede legitimar las intromisiones en otros derechos fundamentales que guarden congruencia con esa finalidad, es decir, que resulten relevantes para la formación de la opinión pública sobre asuntos de interés general.

2.3. Convenios Internacionales.

El Estado español ha ratificado dos Convenios Internacionales que se refieren a la protección de la intimidad o, mejor, de la privacidad de los datos personales [12]. Ambas ratificaciones se han producido con fecha posterior a la de la promulgación de la Constitución Española, por lo que habrá de ser tenido en cuenta lo que en ella se regula bien sea en lo referente a los Derechos y Libertades recogidos en la Sección 1.ª del Capítulo 2.º, como en lo relativo a la posición que ocupan los Convenios Internacionales en nuestro ordenamiento jurídico (arts. 93 a 96 y, sobre todo, el 10.2. CE en lo referido a Derechos Fundamentales).

a) El primero de estos pactos es el Convenio Europeo para protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950, redactado en Roma en el seno del Consejo de Europa y ratificado por España el 26 de septiembre de 1979 (Instrumento publicado en el B.O.E. de 10 de octubre de 1979).

Lógicamente, la fecha de redacción de este Convenio –1950– provoca un evidente desfase en lo relacionado con la regulación de la utilización de la Informática ya que, si resulta evidente que la tecnología ha progresado sustancialmente desde esta fecha, resulta obvio que la aplicación de la Informática al Derecho en general y a la gestión de datos personales en particular ha ido ganando protagonismo en la medida en que los equipos informáticos –hardware– y los programas de gestión –software– han evolucionado, resultando desde hace relativamente pocos años cada vez más operativos a la par que más rentables económicamente.

A pesar de este normal desfase cronológico del Convenio en lo relacionado con la Informática, es de destacar el apartado n.º 2 del artículo 8 en el que, refiriéndose al derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de su correspondencia, se establece:

«No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que en una sociedad democrática sea necesaria para la seguridad

[12] A la distinción entre intimidad –concepto amplio– y privacidad –concepto restringido– se refiere el mismo Proyecto de Ley en el apartaddo I de su exposición de motivos.

nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.»

Este art. 8.2. comienza estableciendo el principio general de la no injerencia por parte de la Administración en la intimidad personal de los ciudadanos para, a continuación, establecer los casos en los que se admiten excepciones a dicho principio general y la reserva de ley para el establecimiento de dichas excepciones y limitaciones [13].

No es aventurado afirmar que el contenido de este art. 8 del Convenio Europeo responde a la misma delimitación material que el art. 18 de la CE, en cuyo apartado 4.º sí se hace una mención expresa al uso de la Informática; el lapso de tiempo de casi tres décadas que separa a un texto del otro (1950-1978) ha permitido la evolución tecnológica que ha desencadenado la existencia hoy de una nueva problemática a la que necesariamente han de responder las normas jurídicas.

En cuanto a la operatividad del Convenio, sucede con su contenido lo que en otros Pactos internacionales en los cuales, al pretender aglutinar a un número amplio de Estados para su ratificación, se pierde concreción en la regulación y, por consiguiente, efectividad práctica del mismo.

Por ello, las excepciones recogidas en este art. 8.2. posiblemente resulten en la práctica en exceso numerosas y difusas, permitiendo así interpretaciones del Convenio que provoquen la impunidad de determinados actos ilícitos que puedan llevar a cabo las Administraciones de determinados Estados firmantes, bien directamente en su actividad habitual (sobre todo en lo referido a la actividad de policía stricto sensu), o bien indirectamente, no evitando la incorrecta actuación de los particulares [14].

b) El segundo Convenio también se redactó bajo los auspicios del Consejo de Europa y su finalidad es, expresamente, la ordenación de la utilización de la Informática en la gestión de los datos personales de los ciudadanos. Es el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio n.º 108), redactado en Estrasburgo el 28 de enero de 1981 y ratificado por España el

[13] Además, en el Convenio se prevé la creación de dos órganos (la Comisión y el Tribunal Europeo de Derechos Humanos) que serán competentes para conocer de las demandas que particulares, asociaciones no gubernamentales o Estados interpongan contra los Estados ratificantes transgresores del Convenio (Títulos II, III y IV).

[14] Recuérdese la ocasión en que la Comisión rechazó una demanda contra la entonces República Federal de Alemania por permitir su legislación la conservación indefinida de las fichas y los antecedentes penales en los ficheros y bancos de datos de los Cuerpos de seguridad del Estado, rechazo que la Comisión fundamentó en la afirmación de que tal posibilidad no era contraria a lo previsto en el Convenio desde el momento en que el apartado 2.º del art. 8 prevé la excepción relativa a la seguridad pública, la defensa del orden y la prevención del delito (GARCÍA DE ENTERRIA, 1983).

27 de enero de 1984, con entrada en vigor el 1 de octubre de 1985 (Instrumento publicado en el BOE de 15 nov. de 1985) [15].

El Convenio se aplica al tratamiento de datos de personas físicas que se realice en el ámbito público o privado, afectando a cualquier tipo de ficheros. El contenido material del Convenio se articula a través de un esquema tripartito:

a) *Disposiciones generales y principios básicos para la protección de datos* (Cap. I y II),

b) *Normas reguladoras del flujo de datos a través de las fronteras* (Cap. III) y

c) *Organización de la ayuda mutua y de las consultas entre las partes.* (Cap. IV y V).

El art. 1 (Cap. I) de dicho Convenio establece bajo la rúbrica «Objeto y fin»:

> «El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos").»

Es interesante comparar, al igual que hicimos con el Convenio Europeo de Derechos Humanos de 1950, lo dispuesto en este art. 1.º con lo previsto en el 18.4. de la CE (anterior cronológicamente). El Convenio matiza lo dispuesto explícitamente por la Constitución, de forma que ya no se trata tanto de «limitar» el uso de la Informática para garantizar al ciudadano la intimidad personal y el ejercicio de sus derechos, como de «garantizar» el respeto de los derechos fundamentales en relación con la gestión informática de los datos personales, incluyendo el derecho a la vida privada; de modo que se hace una inversión de los términos transitando de lo genérico a lo concreto en vez de lo concreto a lo genérico (HEREDERO HIGUERAS, 1.986).

Además, en este Convenio se reitera el mandato dirigido al legislativo establecido en el art. 18.4. CE, en el sentido de que se regule –limite– a través de una Ley la utilización de la Informática en la gestión de datos personales ya que, el art. 4 del Convenio, iniciando el Capítulo II del mismo, establece bajo la rúbrica «Principios básicos para la protección de datos»:

> «1. Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

[15] El Consejo de Europa, además de propiciar la redacción del Convenio n.º 108, ha dirigido desde el año 1985 varias recomendaciones a los Estados miembros en lo relativo a la protección de los datos personales, con un contenido material más concreto: campañas de publicidad directa (1985), datos utilizados por la Seguridad Social (1986), por la Policía (1987), comunicación a terceros de datos en poder de organismos públicos (1991).

2. Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha parte.»

El Capítulo II del Convenio, que comienza con este art. 4, supone la *regulación mínima* que debe ser desarrollada por las normas internas que cada Estado parte dicte después de la ratificación y así, vemos cómo el Proyecto de LORTAD lo que pretende es, al fin, cumplir los compromisos del Estado español, tanto en lo relativo al mandato constitucional contenido en el art. 18.4. CE como al del art. 4 del Convenio de 1981, cubriéndose el vacío legal que supone la inexistencia de un texto que sistematice todas la normas jurídicas referentes al Derecho Informático o, mejor, referentes a la utilización de la Informática en la gestión de los datos personales de los ciudadanos.

En tanto en cuanto que no se promulgue la LORTAD, nuestra regulación actual seguirá siendo escasa, asistemática, y estará dispersa en diversas normas de distinto rango legal y contenido material cada una y, lo que es más peligroso desde el punto de vista de la seguridad y de la efectividad jurídica, se seguirán manteniendo importantes lagunas en el ordenamiento jurídico que provocan la indefensión del ciudadano ante la actuación ilícita de la misma Administración o de organizaciones privadas, que operan en ocasiones como auténticos «delincuentes informáticos», impunes necesariamente por falta de regulación legal o de tipificación que sancione su comportamiento [16].

2.3. Proyectos legislativos españoles.

Desde 1980 hasta hoy se han producido en la actividad parlamentaria numerosísimos actos que tienen como objeto la regulación legal de la utilización de la informática en la gestión de datos personales de los ciudadanos [17]. Estos actos han sido «*preguntas*» dirigidas al Gobierno –orales y escritas–, «*comparecencias*» de distintos ministros –ante el Pleno y en Comisiones–, «*Proposiciones no de ley*» y «*Proposiciones de ley*». Para no desbordar el tema propuesto y por ser los más claros antecedentes de la LORTAD de entre toda la actividad parlamentaria, nos referiremos únicamente a estas últimas [18].

---

[16] No debe confundirse nuestra situación actual con la opción elegida por algunos Estados, prefiriendo una reglulación sectorial, a través de varias normas, en vez de una legislación global, en una sola, ya que ello es fruto de una decisión legislativa racional, y no de la simple falta de previsión.

[17] La primera actividad parlamentaria de este tipo publicada en el Boletín Oficial de las Cortes Geneales data de 1980, y fue una pregunta escrita presentada por el diputado D. Manuel Fraga Iribarne sobre la necesidad de un proyecto de ley de protección de datos o de ordenación y control del uso de la informática. (BOCG del Congreso de los Diputados, Serie F, n.º 1024-I y 1024-II, de 24 de julio y 5 de noviembre de 1980).

[18] a) Proposición de la ley protección al honor y a la intimidad de las personas frente a la utilización de las Bases de Datos, presentada por el Grupo parlamentario de Coalición Popular en el Congreso de los Diputados el día 27 de abril de 1987 (debatida en Pleno y rechazada el día 12 abril 1988).

b) Proposición de ley orgánica para la protección de los derechos y libertades en relación con el uso de la informática y las telecomunicaciones, presentada por el Grupo parlamentario

Distinguimos dos «grupos»: las que son auténticos «proyectos de ley», al acompañarse de un texto articulado cuya aprobación supondría la aparición en el ordenamiento de una nueva norma encargada de regular lo relativo a la protección de datos personales frente al uso de la Informática (todas menos la del Grupo Parlamentario CDS) y las que suponen simplemente la reforma de alguna de las normas ya existentes (la del GP CDS, que pretende la reforma del Código penal, en aras de la tipificación el delito informático a través de la adicción de dos nuevos artículos, el 535 bis y el 535 ter.).

Dentro del primer grupo, todos los Proyectos de ley (es decir, el de Coalición Popular y el de Izquierda Unida) señalan como fundamento de su ser el vacío legal que provoca la inexistencia de una norma jurídica que regule el tratamiento automatizado de los datos personales de los ciudadanos, además de referirse a los mandatos del ya analizado art. 18.4 CE y del art. 4 del Convenio n.º 108 del Consejo de Europa, que veremos posteriormente.

El contenido material de estos dos Proyectos es variado y ambos, en menor o mayor medida, reciben influencias de las legislaciones vigentes de Derecho comparado, anteriores a la presentación material del Proyecto. La distribución de dicho contenido material es distinta, pasando de los aparentemente escasos 10 arts. del Proyecto de Coalición Popular del año 1987 a los 42 artículos del Proyecto de IU-IC de 1988 y de 1989 (El Proyecto gubernamental de LORTAD contiene 48 artículos).

Cada uno de ellos aporta soluciones distintas a los problemas que plantea el uso de la Informática en el tratamiento de los datos personales y únicamente señalaré aquí, como novedad, el órgano de nueva creación que prevé la Proposición de IU-IC: la denominada Comisión Nacional para la telemática y la protección de los derechos y libertades, que podríamos comparar con la Agencia de protección de datos que recogen los arts. 34 y ss. del Proyecto de LORTAD.

3. CONCLUSIONES

Desde hace ya varios años, doctrinalmente se distinguen varias generaciones referidas a los Derechos Fundamentales [19], de tal manera que en el

Mixto-Agrupación Izquierda Unida-Iniciatia per Catalunya en el Congreso de los Diputados el día 23 de junio de 1988 (debatida en Pleno y rechazada el día 14 de abril de 1989).

c) Proposición de ley sobre el delito informático, presentada por el Grupo parlamentario del Centro democrático y Social en el Congreso de los Diputados el día 10 de marzo de 1989 (debatida en Pleno y rechazada el día 23 de junio de 1989).

d) Proposición de ley orgánica para la protección de los derechos y libertades en relación con el uso de la informática y las telecomunicaciones, presentada por el Grupo parlamentario Mixto-Agrupación Izquierda Unida-Iniciatia per Catalunya en el Congreso de los Diputados el día 22 de diciembre de 1989 (debatida en Pleno y rechazada el día 30 de abril de 1990). Este texto y el anterior son idénticos en cuanto a su contenido; simplemente, fueron presentados en dos momentos políticos distintos.

[19] Así, la 1.ª generación de DF sería la nacida de los movimientos sociales revoluciona-

derecho a la intimidad –DF clásico de 1.ª generación– aparece una nueva dimensión como consecuencia de la aplicación de la Informática a la gestión de los ámbitos personal y familiar del individuo.

De la misma forma que distinguimos generaciones en los DF, también se distinguen generaciones en las normas reguladoras de la protección de datos personales –Derecho comparado–. El Proyecto de LORTAD pertenece a la 3.ª generación de este tipo de normas, generación que se habría iniciado con el Convenio n.º 108 del Consejo de Europa (PÉREZ LUÑO, A. E., 1989).

Precisamente, la principal virtud de la LORTAD radica en que, debido a su redacción tardía (las primeras normas aparecieron en Europa en la década de los '70), ha sido posible conocer no sólo la legislación vigente en otros países, sino también su desarrollo y efectividad, es decir, ha sido posible analizar las soluciones propuestas por otros legisladores a problemas similares con una cierta perspectiva, de modo que se han podido adoptar los aciertos y eliminar los defectos.

En cuanto a las características «novedosas» de la LORTAD que nos permiten colocarla dentro de la 3.ª generación, podemos señalar:

–La finalidad, que es, como dice su Exposición de motivos «hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos». Es decir, se trata de asegurar que las garantías de los DF en general y del derecho a la intimidad en concreto no se vean modificadas por la aparición de nuevas técnicas de comunicación, de modo que la estructura «tradicional» de los DF no sea alterada ni, lo que es más importante, reducida respecto de lo que ha sido su normal desarrollo desde el siglo XVIII.

–El establecimiento de los principios de «congruencia» (supone que los datos personales recogidos en ficheros informáticos han de ser veraces –congruentes con la realidad a que se refieren–); de «racionalidad» (supone que los datos sólo podrán ser utilizados para el fin con el que fueron obtenidos

---

rios acaecidos en el siglo XVIII en Norteamérica y, sobre todo, en Europa (Revolución Francesa). Estos DF de 1.ª generación se caracterizan por ser derechos civiles y políticos, es decir, derechos de defensa de la individualidad de la persona frente a la actividad del Estado.

La 2.ª generación de DF aparecería en el primer tercio del s.XX y hallaría su consolidación hacía la mitad del mismo, como reacción a los abusos cometidos por los beligrents en la II Guerra Mundial. En esta generación aparecen los derechos económicos, sociales y culturales y, frente a la 1.ª generación, se caracterizan por ser consecuencia de una nueva concepción de la persona, entendiéndola no sólo como individuo, que garantizan la 'inactividad' del Estado en determinados ámbitos personales, sino que son una exigencia de actividad positiva que un colectivo –el grupo social– dirige al Estado, al que se ve como la cristalización política de dicho grupo.

Si la 1.ª generación de DF es consecuencia del paso del 'Estado absolutista' al 'Estado liberal' y la 2.ª generación lo es del paso del Estado liberal al 'Estado social', la 3.ª generación podríamos afirmar que es hija del 'Estado del bienestar', de modo que la característica de estos derechos es, por una parte, la solidaridad y, por otra, la reacción contra la degraduación paulatina sufrida en este final de siglo por los DF contenidos en las otras dos 'generaciones'.

o solicitados); de «consentimiento» o «autodeterminación» (que suponen, por una parte, la necesidad de que la persona otorgue su consentimiento expreso para la obtención de determinados datos –los denominados «datos sensibles»– y, por otra, la posibilidad de elegir el nivel de protección de que gozan los datos a ella referentes) y los denominados derechos de acceso, de rectificación y de cancelación (posibilidad que tiene toda persona de conocer en cualquier momento los datos contenidos en ficheros informáticos que se refieran a ella y de solicitar la modificación o anulación de los datos que resulten falsos o inexactos).

–La regulación de lo que se ha dado en denominar '«flujos» o «transferencias» internacionales de datos', estableciendo determinados requisitos a cumplir por parte de los Estados receptores exceptuando de dichas transferencias datos con un especial carácter de privacidad –los ya señalados «datos sensibles»–.

Por último, el establecimiento de la Agencia de Protección de Datos; a ella se dedica todo el Título Sexto del Proyecto, y se configura como un órgano administrativo independiente –en la medida en que su Director es nombrado por un plazo de 4 años y no puede ser apartado del puesto sino por causas tasadas legalmente– que está encargado, entre otras funciones, de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación [art. 36, a)], de procurar la cesación de los tratamientos de datos y la cancelación de los ficheros que no se ajusten a la Ley [art. 36, f)], y de ejercer la potestad sancionadora [art. 36, g)].

Como un órgano integrado dentro de la Agencia, se crea el Registro General de Protección de Datos, en el cual se habrán de inscribir, para que su utilización sea lícita, los ficheros, los datos identificativos de los propietarios y usuarios de los mismos, las autorizaciones de uso otorgadas por la Agencia, etc. (art. 38). Es decir, este Registro opera como un cauce de publicidad de los ficheros, de modo que se trata de evitar la indefensión de la persona, primero a través del control de los datos contenidos en los ficheros y, segundo, a través del conocimiento de los responsables del archivo y de la utilización de dicho contenido, canalizándose a través de la Agencia las posibles reclamaciones de los afectados.

BIBLIOGRAFIA

GARCÍA DE ENTERRÍA, E. et al., «El sistema europeo de protección de los derechos humanos. Estudio de la Convención y de la jurisprudencia del Tribunal Europeo de Derechos Humanos», Madrid, *Civitas S. A.*, 2ª ed., 1983, 695 pp., p. 101.

HEREDERO HIGUERAS, M., «La Informática y el uso de la información personal», en AAVV, Introducción a la Informática Jurídica, Actas del Congreso Introducción a la Informática Jurídica, Granada, 8-10 mayo 1985, al

cuidado de RIVERO, A. M. y SANTODOMINGO, A., Madrid, *Fundesco*, 1986, 167 pp., p.38.

LOSANO, M. G., PÉREZ LUÑO, A. E., GUERRERO MATEUS, M. F., «Libertad Informática y leyes de protección de datos personales», Madrid, Centro de Estudios Constitucionales, 1989, 213 pp., p. 148 y 149.

MESA N.º 3.–PROTECCION DE DATOS III.
(Situación Internacional)

El Derecho a la autodeterminación informativa en la ley portuguesa de protección de datos de 1991. Sujetos, contenido y garantías

JOSE M.ª ASPAS ASPAS
Licenciado en Derecho
Administrador Superior
Diputación General de Aragón
(ESPAÑA)

SUMARIO

I. LA CONSTITUCIONALIZACION DE LA PROTECCION DE DATOS FRENTE A LA INFORMATICA
II. EL DESARROLLO LEGISLATIVO DEL ARTICULO 35 DE LA CONSTITUCION PORTUGUESA
1. El retraso legislativo. Compromisos internacionales.
2. La Ley 10/91. La Ley de protección de datos personales frente a la informática.
III. EL DERECHO A LA AUTODETERMINACION INFORMATIVA EN LA LEY PORTUGUESA DE PROTECCION DE DATOS PERSONALES
1. Elementos subjetivos.
A) Sujeto activo.
B) Sujeto pasivo.
2. Contenido.
A) Recogida de datos.

B) Almacenamiento y tratamiento automatizado de datos.

C) Transmisión.

D) Obligaciones del sujeto pasivo.

3. Garantías.

A) Garantías institucionales. La CNPDPI.

B) Delitos y sanciones.

I. LA CONSTITUCIONALIZACION DE LA PROTECCION DE DATOS FRENTE A LA INFORMATICA

El artículo 35 de la Constitución de la República de Portugal de 1976 (CRP) establece lo siguiente:

«1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.

2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.

3. Queda prohibida la atribución de un número nacional único a los ciudadanos» [1].

De este modo Portugal es el primer Estado europeo que constitucionaliza la protección de datos personales frente al uso de la informática [2]. El derecho de acceso, el derecho a conocer la finalidad a la que se destinan los datos, el derecho de rectificación, la prohibición de captar datos sensibles y la prohibición del número de identificación personal único son elementos de la técnica de protección de datos personales conocidos en la legislación comparada de protección de datos [3] de los

---

[1] 1 Citamos por la traducción de M. DARAMAS publicada en el *Boletín de Legislación Extranjera*, núm. 206 (1976), reproducida por J. DE ESTEBAN: *Constituciones españolas y extranjeras,* Taurus, 2.ª ed., Madrid, 1979.

[2] Sobre el artículo 35 de la Constitución portuguesa vid. R. CAPELO DE SOUSA: «A Constituçao e os direitos da personalidades» en la obra colectiva *Estudos sobre a Constituçao, II,* Lisboa. 1978, pp. 194 y ss. y J. J. GOMES CANOTILHO y V. MOREIRA: *Constituçao de Republica Portuguesa. Anotada,* Coimbre Editora, 1980, pp. 103-104.

[3] La expresión «protección de datos es una importación de la terminología alemana *(Datenschutz)* y anglosajona *(Data protection)* con aceptación entre la doctrina española y comparada. Con ella se alude a las normas jurídicas de diverso rango (internacional, constitucional, legal o reglamentario) cuya finalidad es la tutela de bienes jurídicos o derechos de las personas que puedan ser afectados por la elaboración informática de informaciones referentes a personas. Es, por tanto, una expresión equívoca, porque estas disposiciones pretenden proteger a las personas concernidas por los datos, pero no son objeto de protección jurídica los datos por sí mismos. Sobre la cuestión terminológica *cfr.* A. E. PÉREZ LUÑO: «Los derechos humanos en la sociedad tecnológica» en M. G. LOSANO, A. E. PÉREZ LUÑO, Mª F. GUERRERO MATEUS, *Libertad informá-*

años setenta, pero que con su constitucionalización ejercerán una influencia sobre otros sistemas jurídicos [4].

Con el reconocimiento de esa serie de facultades a los ciudadanos para la protección de su identidad informativa, la Constitución portuguesa no constitucionaliza *expressis verbis* el derecho a la autodeterminación informativa,[5] pero lo dota de un contenido mínimo o esencial que no puede ser ignorado por el legislador ordinario.

II. EL DESARROLLO LEGISLATIVO DEL ARTICULO 35 DE LA CONSTITUCION

1. El retraso legislativo. Compromisos internacionales.

Quince años han transcurrido entre la aprobación de la Constitución y el desarrollo legislativo de su art. 35. En efecto, la Ley 10/91, *Ley de protección de datos personales frente a la informática* (LPDP), publicada en el Diario de la República, I Serie-A, n.º 98, de 29 de abril de 1991, llena el vacío legislativo del ordenamiento jurídico portugués en materia de protección de los datos personales [6].

La Ley portuguesa de 1991 debe su aprobación a dos compromisos internacionales. En primer lugar, el *Convenio para la protección de las personas*

---

tica y leyes de protección de datos personales, CEC, Madrid.1989.

[4] El art. 35 CRP es el antecedente del art. 18.4 de la Constitución española. *Vid* J.M. SERRANO ALBERCA: «Comentario al art. 18», en F. GARRIDO FALLA, *Comentarios a la Constitución, Civitas,* 2.ª ed., Madrid, 1985, pp. 351—381 y J. GALVEZ MONTES: «Derecho al honor, a la intimidad y a la propia imagen. Comentario al art. 18 de la Constitución, en O. ALZAGA, *Comentarios a las leyes políticas. Constitución española,* t. II, Edersa, Madrid, 1984.

[5] El derecho a la autodeterminación informativa o libertad informática es una construcción jurisprudencial y doctrinal. Fue enunciado por el Tribunal constitucional alemán (sentencia de 15 de diciembre de 1983, sobre la Ley del censo de 31 de marzo de 1982) hay traducción castellana BJC 33 (1984), pp. 126 y ss como un derecho ligado al derecho a la personalidad (art. 2.1 GG). La doctrina ha intentado configurarlo como un derecho autónomo, correspondiente a la tercera generación de derechos fundamentales. *Vid* A. E. PÉREZ LUÑO: «Libertad informática y derecho a la autodeterminación informativa» en AA.VV., *Congreso sobre Derecho Informático. Texto de ponencias y comunicaciones. Edición previa,* 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, pp. 359-376. También P. LUCAS MURILLO DE LA CUEVA: *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática,* Tecnos, Madrid, 1990.

[6] Tras la aprobación de la Ley portuguesa, en ámbito de los países europeos, sólo carecen de ley de protección de datos tres países: España, Italia y Portugal. En caso de España, se encuentra muy avanzada la tramitación parlamentaria del *Proyecto de Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal (BOCG-CD,* Serie A,núm. 59-1, de 24-7-1991 y *BOCG-S,* Serie II núm. 80(a), de1-6-1992). Italia carece de una ley específica de protección de datos; se han planteado diversas propuestas para colmar esta laguna, de las que da noticia M. G. LOSANO: «Un proyecto de ley sobre la protección de los datos personales en Italia, en M. G. LOSANO, A. E. PÉREZ LUÑO, M.ª F. GUERRERO MATEUS, *Libertad informática y leyes de protección de datos personales, cit.,* pp. 61-94.

con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. El Convenio 108 del Consejo de Europa vincula a los Estados que lo han ratificado, aceptado o aprobado[7].

En segundo lugar, el *Convenio de aplicación del Acuerdo de Schengen* de 14 de junio de 1985 entre el Benelux, Alemania y Francia, *relativo a la supresión gradual de controles en las fronteras comunes*, firmado en Schengen el 19 de junio de 1990,[8] al cual se adhirió, en junio de 1991, Portugal. La adhesión le obligaba a adoptar, antes de la ratificación, todas las iniciativas necesarias para que la legislación portuguesa fuese completada de conformidad con el Convenio 108 del Consejo de Europa.

El Convenio de aplicación del Acuerdo establece en su título IV (arts. 92-119) un sistema de información común, denominado *Sistema de Información de Schengen.* Este sistema consiste en la creación y mantenimiento de un fichero de datos por cada parte contratante y la creación de una unidad de apoyo técnico, que haga posible la consulta automatizada de datos sobre personas y objetos para la aplicación de las disposiciones relativas a la circulación de las personas. Además, se establecen disposiciones sobre la protección de datos de carácter personal (arts. 126-130). Las partes contratantes se obligan a adoptar las disposiciones nacionales que sean necesarias para conseguir un nivel de protección de los datos de carácter personal que sea, al menos, igual al que se desprende de los principios del Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (art. 126.1), sin que puedan transmitirse datos de carácter personal, según el Convenio, hasta que las disposiciones de protección de datos hayan entrado en vigor en el territorio de la parte contratante afectada por la transmisión (art. 126.2).

En nuestra opinión, la adhesión de Portugal al Convenio de aplicación del Acuerdo de Schengen es la causa inmediata del desarrollo legislativo de

---

[7] En 1988, de los veintiún Estados miembros del consejo de Europa, ocho habían ratificado el Convenio 108 (Austria, Francia, España, Luxemburgo, Noruega, R.F. de Alemania y Suecia); otros diez habían expresado mediante su firma su voluntad de ratificarlo (Bélgica, Chipre, Dinamarca, Grecia, Irlanda, Italia, Islandia, Países Bajos, Portugal y Turquía). *Vid* S. RIPOL CARULLA: «El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: balance a los siete años de su apertura a la firma» en AA.VV., *Congreso sobre Derecho informático. Texto de ponencias y comunicaciones. Edición previa*, 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, pp. 395-413.

[8] El texto del Convenio de aplicación de 1990 del Acuerdo de Schengen puede consultarse en el *BOCG-CD,* Series C, núm.194-1 de 26-10-1991. Además de los cinco Estados iniciales, forman parte Italia, que se adhirió en noviembre de 1990 y, España y Portugal, que se adhirieron en junio de 1991; Grecia participa desde enero de 1992 como observador. Sobre el citado Acuerdo, *cfr.* J. L. CORCUERA: «Las fronteras de la Comunidad Europea» y J. ELORZA: «Libre circulación de personas», ambos trabajos publicados en AA.VV., *El mercado único. La Europa sin fronteras interiores,* Acción Institucional 93. Secretaría de Estado para las Comunidades Europeas, Madrid, 1992, pp. 111-119 y 131-141, respectivamente.

la protección de datos prevista en el art. 35 de la Constitución, demorado durante tres lustros.

Como hemos señalado, el Convenio de aplicación del Acuerdo de Schengen establece como parámetro de la protección de los datos personales los principios del Convenio 108 del Consejo de Europa. LUCAS MURILLO DE LA CUEVA ha sintetizado dichos principios, aplicables al sector público y privado, en los siguientes: principio de lealtad, de exactitud, finalista (que comprende los principios de pertinencia, de utilización no abusiva, del derecho al olvido), de publicidad, de acceso individual, de seguridad, la prohibición de tratar informáticamente datos sensibles, salvo que el Derecho interno prevea garantías adecuadas, el establecimiento de recursos y sanciones para garantizar los anteriores principios y, por último, la prohibición de transmitir datos personales a países que no les den una protección equivalente[9].

2. La Ley 10/91. Ley de protección de datos personales frente a la informática.

La LPDP tiene una extensión de 45 artículos, distribuidos en nueve capítulos. El principio inspirador de la regulación de la Ley es el establecimiento de un sistema *preventivo* frente a los riesgos que comporta el uso informático de datos personales sin un control por las personas concernidas por ellos [10]. Las actividades de captación, conservación, tratamiento y transmisión automatizada de datos personales sólo pueden hacerse de acuerdo con las previsiones de la Ley. Es decir, no es un régimen jurídico de libertad incondicionada, sino que la Ley fija el régimen preciso al que deben someterse los agentes que utilizan la informática [11].

La precisión técnica implica la necesidad de incorporar definiciones legales. Así el art. 2 de la LPDP define lo que se entiende, a efectos legales, por datos personales, datos públicos, sistema informático, fichero automatizado, base de datos, banco de datos, tratamiento automatizado, responsable de los soportes informáticos, flujo de datos transfronterizos [12]. Quizás la Ley

---

[9] P. LUCAS MURILLO DE LA CUEVA: *El derecho a la autodeterminación informativa, cit. pp. 141-144.* También A. E. PÉREZ LUÑO «Los derechos humanos en la sociedad tenológica», *cit.* pp. 163-184.

[10] A juicio de M. HEREDERO HIGUERAS es más eficaz un sistema preventivo de actuación que un sistema *ex post facto*, aunque también es posible éste. *Vid.* «Ante la ratificación del Convenio de protección de datos del Consejo de Europa», DA 199 (1983), p. 762 y «El anteproyecto de ley orgánica de regulación del uso de informática, cinco años después» en AA.VV., *Congreso sobre Derecho informático. Texto de ponencias y comunicaciones. Edición previa,* 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, p. 276.

[11] *cfr.,* p. ej., los arts. 17 (requisitos de creación de ficheros automatizados), 24 (interconexión de datos personales) y 33 (flujo transfronterizo de datos). P. LUCAS MURILLO DE LA CUEVA defiende que el principio inspirador de una ley de protección de datos debe ser la fijación de un marco jurídico preciso.*Vid.* «La protección de los datos personales ante el uso de la informática, *RFDUC* 15 (1990), p.615 y *El derecho a la autodeterminación informativa, cit, pp.178-179.*

[12] *Cfr.,* el art. 2 del Convenio 108 del Consejo de Europa. Las definiciones del Convenio sólo se refieren a datos de carácter personal, ficheros automatizados, tratamiento automatizado,

no debería hacer referencia expresa a las locuciones «banco de datos», «base de datos» o «sistema informático», ya que son conceptos que están vinculados a un determinado estadio del desarrollo informático y de la evolución tecnológica de la informática [13].

Como hemos señalado *supra*, el art. 35 de la Constitución no recoge el bien jurídico protegido, es decir, la autodeterminación informativa, sino diversas técnicas de protección de datos. Sin embargo, la LPDP, al señalar el objeto y fin de la regulación, ha precisado el bien jurídico protegido. El art. 1 de la Ley establece:

«El uso de la informática debe procurarse de forma transparente y con estricto *respeto* a la *reserva de la vida privada y familiar* y de los *derechos, libertades y garantías fundamentales* del ciudadano.»

Este artículo no se refiere exclusivamente a la reserva personal y familiar (o intimidad), sino también a los derechos, libertades y garantías fundamentales de los ciudadanos. Además de la intimidad personal y familiar hay otros bienes jurídicos que deben tenerse en cuenta. La autodeterminación informativa como derecho fundamental autónomo guarda relación de complementariedad con otros derechos y libertades fundamentales, como son la de conciencia, religión y culto (art. 41 CRP), la de expresión y de información (art. 37).

El bien jurídico protegido es la identidad informativa, manifestación de la *identidad de la persona.*[14] Lo que se protege es el control de la utilización y tratamiento automatizado de datos personales por las personas afectadas.

Es importante destacar la perspectiva que adopta la LPDP: lo que se regula es el uso de la informática (art. 1). Este enfoque ya estaba presente en el art. 35 de la Constitución, que lleva por título «*Utilización de la informática*». Se pretende resolver el conflicto entre la libertad de utilizar sistemas automáticos de almacenamiento, tratamiento y transmisión de datos personales y la libertad informática o autodeterminación informativa. Por ello, se regula el uso, sometiéndolo al régimen legal que configura el *status* de *habeas data*[15], concretado en las garantías o derechos de acceso y control de las informaciones procesadas informáticamente por las personas concernidas.

---

autoridad controladora del fichero. La LPDP ha incluido, además, las definiciones de los datos públicos, sistema informático, base de datos, banco de datos y flujo transfronterizo.

[13] El término «fichero automatizado», que es el que utiliza el Convenio europeo, bastaría para englobar los conceptos de base y banco de datos. Esta simplificación terminológica haría menos redundante el texto de la Ley, ya que en la mitad de sus artículo en –concreto en los arts. 3, 8, 13, 14, 17, 18, 20, 21, 24, 25, 26, 27, 29, 32, 34, 35, 36, 37, 39, 40, 41, 44, y 45– se repite la expresión «fichero de datos, base de datos y banco de datos».

[14] M. HEREDERO HIGUERAS («Ante la ratificación del Convenio de protección de datos del Consejo de Europa». *cit.*, p. 762) sostiene que lo que debe ser protegido por las leyes de protección de datos es «la integridad de la información personal, en cuanto que es expresión de la identidad de la persona. El tráfico incontrolado de la información personal puede dar lugar a distorsiones o alteraciones de la identidad de las personas».

[15] Sobre el *habeas data vid.* A. E. PEREZ LUÑO: «Del *habeas corpus al habeas data*»

III. ELEMENTOS DEL DERECHO A LA AUTODETERMINACION INFORMATIVA EN LA LEY PORTUGUESA DE PROTECCION DE DATOS PERSONALES

El derecho a la autodeterminación informativa es una posición jurídica subjetiva que corresponde al *status* de *habeas data*. Es, valga la redundancia, un derecho subjetivo, configurado por la Constitución y por la Ley de protección de datos personales de 1991.

1. Elementos subjetivos.

El derecho a la autodeterminación informativa implica la existencia de una relación jurídica con dos sujetos o posiciones: la del titular del derecho (posición activa) y la de los obligados (posición pasiva).

A) Sujeto activo.

El titular del derecho a la autodeterminación informativa es, en primer lugar la *persona física. La dicción literal del artículo 35 de la Constitución plantea un problema al limitar la protección a los ciudadanos* («Todos los ciudadanos...»). La Ley, siguiendo la senda constitucional, refiere el derecho a la autodeterminación informativa a los ciudadanos (art. 1). No obstante, hay que entender que la protección se extiende a los *extranjeros*, como titulares del derecho, en virtud del art. 15 de la Constitución, ya que ni ésta ni la Ley han reservado este derecho exclusivamente a los ciudadanos portugueses [16].

En segundo lugar, también son titulares del derecho las *personas jurídicas*, siempre que los ficheros, bases o bancos de datos contengan datos personales. Así resulta del art. 3.1.b) de la Ley, que dice: «Las disposiciones de la presente Ley se aplicarán obligatoriamente: (...) a los soportes informáticos relativos a personas jurídicas y entidades equiparadas, siempre que contengan datos personales». El Convenio del Consejo de Europa se refiere a las personas físicas (art. 1), pero deja abierta la posibilidad de que los Estados miembros puedan extender el régimen de protección a las personas jurídicas (art. 3.b.). Esta extensión de la titularidad del derecho a la autodeterminación informativa a las personas jurídicas, que ha efectuado el legislador portugués, es una clara manifestación de que el bien jurídico protegido no es exclusivamente la intimidad personal o familiar, ya que ésta en sentido estricto, sólo podría referirse a las personas físicas y a los miembros individuales de las personas jurídicas [17].

---

en AA.VV., *Encuentros sobre informática y Derecho 1990-1991,* Universidad Pontificia de Comillas, Madrid, 1992, pp.171-179.

[16] El art. 15 CRP dispone: «1. Los extranjeros y los apátridas que se encuentren o residan en Portugal gozarán de los derechos y estarán sujetos a los deberes del ciudadano portugués. 2. Quedan exceptuados de los dispuesto en el número anterior (...) los derechos y deberes reservados por la Constitución y por la ley a los ciudadanos portugueses».

[17] Sobre el problema de las personas jurídicas *vid* P. LUCAS MURILLO DE LA CUEVA «La

B) Sujeto pasivo.

El sujeto pasivo del derecho a la autodeterminación informativa configurado por la LPDP es toda *persona física o jurídica, pública o privada*, que utilice sistemas de almacenamiento y tratamiento automatizado de datos personales.

La extensión de la posición pasiva deriva del art. 17 de la Ley que, al determinar los requisitos a los que está sujeta la creación de ficheros automatizados, bases o bancos de datos, somete al régimen legal a todos los sujetos que creen ficheros, sean entidades públicas o privadas. Las amenazas a la identidad informativa pueden proceder del sector público y también del sector privado; por ello, el derecho a la autodeterminación informativa no se configura como un derecho público subjetivo, sino como un derecho subjetivo en el que pueden ocupar la posición de deber las personas públicas y las privadas.

El *ámbito de aplicación* de la LPDP delimitado en su art. 3 determina que a su régimen legal se sujeten únicamente los ficheros automatizados, quedando excluidos los manuales. Además, se excluyen una serie de supuestos en los que media el consentimiento implícito de la persona concernida (procesamiento de remuneraciones, facturación de suministros, cobro de cotizaciones) y los ficheros que contienen datos personales destinados a mantener la seguridad pública (Sistema de Información de la República). También se excluyen los ficheros que contengan informaciones destinadas al uso personal. Respecto a los datos relacionados con la seguridad pública, el art. 9.2 del Convenio 108 del Consejo de Europa permite dicha exclusión.

2. Contenido del derecho.

El contenido del derecho a la autodeterminación informativa se desprende de las facultades que la LPDP atribuye al sujeto activo para proteger su identidad informativa. Es el conjunto de derechos subjetivos que permiten al sujeto activo definir la intensidad con la que desea que sea conocida su identidad informativa, circulen sus datos y que, además, le permitan defenderse de los abusos, inexactitudes o uso desviado que de los mismos se haga, bien sea en el momento de su recogida, tratamiento, almacenamiento o transmisión.

A) Recogida de datos.

El art. 22 de la Ley establece que la recogida de datos personales debe hacerse mediante un *documento o cuestionario, en el que debe constar que los datos serán procesados automáticamente, si es obligatorio o facultativo*

---

protección de los datos personales ante el uso de la informática, *cit.* pp. 617-618 y la reelaboración posterior, *El derecho a la autodeterminación informativa, cit.* pp. 181-182, en la que modifica su criterio.

proporcionar los datos, las consecuencias en caso de omisión o inexactitud de las respuestas, los destinatarios de las informaciones, su finalidad, la identificación del responsable del fichero y su dirección y las condiciones del ejercicio del derecho de acceso. Sin embargo, estos requisitos no se exigen en la recogida de datos destinados a la prevención de delitos o con fines estadísticos (art. 22.2).

Esencial en la técnica de protección de datos referida a su captación es la prohibición de recoger *datos personales sensibles*. Esta prohibición es un mandato del art. 35.2 de la Constitución y ha sido completada por el art. 11 de la Ley. La Constitución prohíbe el tratamiento automatizado de datos referentes a las convicciones políticas, fe religiosa o vida privada. A estas categorías de datos la Ley ha añadido las referidas a la filiación política o sindical (art. 11.1.a.) y al origen étnico, condenas penales, sospechas de actividades ilícitas, estado de salud y situación patrimonial y financiera (art. 11.1.b.).

La prohibición constitucional pese a la rotundidad de los términos en los que está formulada, no debe entenderse de una forma absoluta. Así lo ha interpretado el legislador, que permite el tratamiento de los datos sensibles si media el consentimiento previo de sus titulares, con el conocimiento por éstos del destino y utilización de los datos (art. 11.4).

Por otra parte, el tratamiento de datos sensibles enumerados en la letra b) del art. 11.1 (esto es, los añadidos por la Ley) puede ser efectuado por los servicios públicos, siempre que se respete el régimen legal y se cuente con el parecer de la Comisión Nacional de Protección de los Datos Personales Informatizados (art. 11.3), que la Ley crea.[18] Por lo tanto, se establece una «escala de informaciones sensibles».

Si los datos sensibles no son identificables pueden ser objeto de tratamiento automatizado para fines de investigación o estadísticos (art. 11.2). Esta modulación o relativización de la prohibición es consecuencia de dos hechos: uno, que los datos sensibles dejan de serlo si no es identificada o identificable la persona a la que se refieran; es más, dejan de ser, a efectos legales, datos personales (*cfr.* la definición de los datos personales de la letra a) del art. 2 LPDP); el otro hecho es que la perspectiva de la legislación de protección de datos es regular la utilización de la información, de ahí que determinados usos (investigación científica o estadística) sean permitidos.

En la recogida de datos rige el principio de calidad de los datos, reconocido en el art. 5 del Convenio 108 del Consejo de Europa. Así, los datos personales que sean objeto de tratamiento automatizado deben cumplir los requisitos de: *lealtad*, la recogida debe efectuarse de forma lícita y no engañosa (art. 12.1 LPDP); *finalidad*, la finalidad determinante de la recogida

[18] A la CNPDPI nos referiremos *infra*§III.3.A).

debe ser conocida antes de su inicio (art. 12.3); *pertinencia*, la recogida debe procesarse con estricta adecuación y pertinencia a la finalidad que se determine (art. 12.2); y, *exactitud*, los datos personales recogidos y mantenidos en ficheros automatizados deben ser exactos y actuales (art. 35.1 CRP y art. 14 LPDP).

B) Almacenamiento y tratamiento automatizado de datos.

El sujeto activo del derecho a la autodeterminación informativa goza de una serie de derechos para defender su posición. Así,

a) El *derecho a conocer la existencia* de bancos de datos. El art. 13 LPDP establece que cualquier persona tiene el derecho de ser informada sobre la existencia de un fichero automatizado, base o banco de datos personales que le afecten, de la respectiva finalidad, así como sobre la identidad y la dirección del responsable. Es un principio paralelo al recogido en el art. 8 del Convenio del Consejo de Europa.

b) El *derecho de acceso* a la información personal. Todas las personas, debidamente identificadas, tienen reconocido el derecho de acceso a las informaciones sobre ellos registradas (art. 35.1 CRP y art. 27 LPDP) con las excepciones de la legislación sobre secretos del Estado y de la Justicia. El ejercicio de este derecho no puede ser limitado, aunque puede someterse a reglas para evitar un ejercicio abusivo (art. 28.1 LPDP). El Convenio 108 del Consejo de Europa exige que las peticiones de acceso se puedan formular a intervalos razonables y sin demora o gastos excesivos (art. 8.b.); en la legislación comparada, por ejemplo, se autoriza al sujeto pasivo a exigir el pago de un canon razonable. La información debe ser comunicada de forma inteligible. Dispone el art. 28.2 LPDP que la información debe ser transmitida en lenguaje claro, exenta de codificaciones y debe corresponder rigurosamente al contenido del registro. En el caso de información médica, el acceso es indirecto, ya que la información debe ser comunicada por medio de un médico designado por la persona interesada (art. 28.3).

c) Los *derechos de rectificación, integración y cancelación.* Consecuencia del ejercicio del derecho de acceso puede ser el de estos derechos para asegurar la calidad de los datos, de la que es uno de sus presupuestos la exactitud y actualidad de los datos.

Así, según el art. 30.1 LPDP, cualquier persona tiene derecho a exigir la corrección de las informaciones inexactas que le afecten (derecho de rectificación) y a que se completen las omitidas total o parcialmente (derecho de integración). La carga de la prueba de la inexactitud corresponde al titular del registro cuando la información hubiera sido proporcionada por él mismo o con su consentimiento o si no hubiere comunicado su alteración (art. 30.2).

La LPDP reconoce, igualmente, el derecho de cancelación expresamente. Cualquier persona tiene derecho a la supresión de las informaciones personales que se tengan en ficheros automatizados y que hayan sido obteni-

das por medios ilícitos o engañosos o cuyo registro o conservación no sean permitidos (art. 30.1. *in fine*). En el sistema de la Ley rige el principio de limitación temporal de conservación de los datos: los datos pueden conservarse sólo el tiempo estrictamente necesario para su finalidad. Así, el responsable del fichero está obligado a destruir los datos una vez transcurrido el plazo de conservación autorizado (art. 23), ya que los ficheros se crean por tiempo determinado (*cfr.*, el art. 18.i, que exige que en la solicitud de informe o autorización para crear un fichero automatizado debe figurar el tiempo de conservación de los datos personales). Por otra parte, la destrucción de datos puede ser ordenada por la CNPDPI (art. 8.1.g en relación con los arts. 20 y 23). Una manifestación concreta del derecho de cancelación es el derecho reconocido a cualquier persona para exigir que su nombre y dirección sean eliminados de ficheros de direcciones utilizadas para el *marketing* directo o *mailing* (art. 30.3).

Un aspecto importante del tratamiento automatizado de datos es el referido a su uso. El art. 15 LPDP, a este efecto, dispone que los datos personales sólo pueden ser utilizados para la finalidad determinante de su recogida, salvo autorización concedida por ley. Ya nos hemos referido más arriba al uso de datos en los trabajos de investigación o con fines estadísticos –uso en forma anónima, salvo consentimiento expreso del interesado– (art. 11.2 y 11.4); prohibición de utilizar perfiles de personalidad obtenidos como resultado de un tratamiento automatizado de información como fundamento único de decisiones judiciales, administrativas o disciplinarias (art. 16). También nos hemos referido con cierto detalle a la prohibición y restricciones del tratamiento automatizado de datos personales sensibles (art. 11).

C) Transmisión de datos.

En relación con el uso de los datos personales destaca el tema de la interconexión de *ficheros automatizados*. La regla general es la prohibición de interconectar datos personales (art. 24.1). Excepcionalmente se permite la interconexión de datos públicos –esto es, los que constan en un documento público oficial, exceptuados los elementos confidenciales– entre entidades que persigan los mismos fines específicos (art. 25). La regla general puede ser exceptuada mediante ley, que deberá definir expresamente los tipos de interconexión autorizados y su finalidad (art. 26). En cualquier caso, esta utilización conjunta de ficheros automatizados que contengan datos personales debe ser autorizada preceptivamente por la CNPDPI (art. 8.1.d.).

Una cuestión íntimamente relacionada con la interconexión de ficheros automatizados es la de la atribución de un *número de identificación personal único* [19]. El art. 24.2 LPDP dice literalmente que «no está permitida la atribu-

[19] En España la creación del número de identificación fiscal (NIF) por el art. 113 de la Ley 33/1987, *de 23 de diciembre, de Presupuestos Generales del Estado para 1988, desarrollado por el Real Decreto 338/1990, de 9 de marzo,* ha suscitado la cuestión sobre si es compatible la atribución de un número nacional único a cada persona con el derecho a la autodeterminación

ción de un número ciudadano para interconectar ficheros automatizados de datos personales que contengan informaciones de carácter policial, criminal o médico». *Sensu contrario* cabría atribuir un número de identificación personal para interconectar ficheros automatizados de datos personales que contengan cualesquiera otras informaciones que no fuesen de carácter policial, criminal o médico. Esta interpretación no es correcta ya que la Constitución contiene una prohibición absoluta de atribuir un número de identificación personal único en su art. 35.3: «Queda prohibida la atribución de un número nacional único a los ciudadanos». En otro caso, habría que reputar inconstitucional el art. 24.2 de la Ley por vulnerar el art. 35 de la Norma fundamental.

El problema del *flujo transnacional de datos* es abordado por la LPDP en su art. 33, que concuerda con el art. 12 del Convenio del Consejo de Europa. El intercambio internacional de datos queda sometido al régimen general de la Ley (art. 33.1). Además, se establece el principio de «protección equivalente»: la CNPDPI puede autorizar flujos transfronterizos de datos si el Estado de destino garantiza una protección equivalente a la de la Ley (art. 33.2). Por último, se prohíbe el flujo transnacional si con ello se pretende eludir las prohibiciones o condiciones de la Ley o hacer posible la utilización ilícita de los datos (art. 33.3)[20].

D) Obligaciones del sujeto pasivo.

El conjunto de derechos del sujeto activo del derecho a la autodeterminación informativa vincula a los sujetos pasivos, que están sometidos a obligaciones genéricas y específicas.

Las obligaciones *genéricas* del responsable de los ficheros o soportes informáticos –definido en el art. 2.h.– son la reserva y la garantía de la seguridad de los datos. Los responsables de los ficheros automatizados, así como las personas que, en ejercicio de sus funciones, tengan conocimiento de los datos personales en ellos registrados, están obligados al *sigilo profesional*, durante y al término de sus funciones (art. 32.1), sin que suponga vulneración de este deber de sigilo el proporcionar las informaciones obligatorias de

---

informativa. Para P. LUCAS MURILLO DE LA CUEVA (*El derecho a la autodeterminación informativa, cit* pp. 188-192) el NIF por sí sólo no perjudica ni al derecho a la intimidad ni al derecho a la autodeterminación informativa, aunque puede permitir la lesión de los derechos fundamentales, especialmente si se generaliza su uso en las relaciones privadas. Por contra, para S. A. BELLO PAREDES, el art. 113 de la Ley 38/1987, entendiendo como habilitación general e ilimitada a la Administración tributaria para que reglamentariamente regule la utilización del NIF en la forma y manera que estime más conveniente, debe ser considerada fundamentalmente inconstitucional. *Vid* EL NIF. «Algunas consecuencias de su incardinación en nuestro ordenamiento jurídico» en AA,VV., *Encuentros sobre informática y Derecho 1990-1991,* Universidad Pontificia de Comillas, Madrid, 1992, pp. 159-170.

[20] El flujo transnacional de datos personales es la base sobre la que descansa el Sistema de Información de Schengen (cfr. los arts. 92-119 y 126-130 del Convenio de 1990). En general, sobre el flujo internacional de datos, *vid.* A. E. PÉREZ LUÑO: *Nuevas tecnologías, Sociedad y Derecho. El impacto socio-jurídico de las nuevas tecnologías de la información,* Fundesco, Madrid 1987, pp. 87-90.

acuerdo con las leyes (art. 32.2). La obligación de la *seguridad de los datos* implica que el responsable debe adoptar las cautelas frente al acceso indebido de terceros o alteraciones fortuitas. El art. 21 establece que los ficheros automatizados deben estar equipados con sistemas de seguridad que impidan la consulta, modificación, destrucción o adición de los datos por persona no autorizada a hacerlo y que permitan detectar desvíos de información intencionados o no. Este artículo concuerda con el art. 7 del Convenio del Consejo de Europa.

Las obligaciones *específicas* son las generadas por derechos subjetivos del sujeto activo del derecho a la autodeterminación informativa.

3. Garantías.

A) Garantías institucionales.

El eje de la Ley es la creación de un órgano de control de la aplicación de la Ley, denominado *Comisión Nacional de Protección de Datos Personales Informatizados* (CNPDPI), al que dedica su capítulo II (arts. 4 a 10), además de otros preceptos dispersos en los que se le atribuyen competencias en concreto.

Frente a la opción por un órgano unipersonal (los comisarios alemanes de datos, federal o territoriales, el inspector de datos sueco, el registrador británico) o por un órgano colegiado (la Comisión Nacional de la Informática y de las Libertades francesa), la Ley portuguesa opta por el modelo francés.

La CNPDPI es un órgano colegiado compuesto por siete miembros, de elección inter-poderes: tres (el presidente y dos vocales) son elegidos por la Asamblea; otros dos vocales son magistrados, uno juez elegido por el Consejo Superior de la Magistratura, el otro fiscal elegido por el Consejo Superior del Ministerio Público; y, los dos restantes vocales, han de ser personas de competencia reconocida, designados por el Gobierno (art. 5).

Lo decisivo de la posición de la CNPDPI es su autonomía efectiva frente a los poderes públicos: es una *autoridad administrativa independiente* [21]. Así la califica el art. 4.2: «La CNPDPI es una entidad pública independiente con poderes de autoridad, que funciona junto a la Asamblea de la República y dispone de servicios propios de apoyo técnico y administrativo». La dispo-

[21] Sobre la Administración independiente o neutral *vid.* J. M. SALA ARQUER: «El Estado neutral. Contribución al estudio de las Administraciones independientes», REDA 42 (1884), pp. 401-422; F. J. JIMÉNEZ DE CISNEROS CID: *Los organismos autónomos en el Derecho público español: tipología y régimen jurídico,* INAP, Madrid, 1987, pp. 307-340; A. JIMÉNEZ-BLANCO: *Derecho público del Merecado de Valores,* Centro de Estudios Ramón Areces, Madrid, 1989, pp. 92-107; F. LÓPEZ RAMÓN: «El Consejo de Seguridad Nuclear: un ejemplo de Administración independiente», RAP 126 (1991), pp. 189-216. En la doctrina francesa C.-A. COLLIARD y G. TINSIT (dir): *Les autorités admininistratives indépendantes,* PUF, París, 1988, especialmente el estudio del presidente de la CNIL, J. FAUVET, «La Commission nationale de l'informatique et des libertés», pp.146-149.

nibilidad de medios personales y materiales propios para desempeñar su cometido es un aspecto importante para garantizar su autonomía funcional.

La elección o designación de los miembros de la CNPDPI por los poderes legislativo, judicial y ejecutivo es, igualmente una garantía de su independencia. Esta se ve reforzada por la duración de su mandato, cinco años (art. 10.2) que supera la del mandato del Parlamento y del Gobierno (cuatro años, art. 174 CRP).

Ahora bien, lo determinante de su posición independiente es el conjunto de potestades que la Ley le atribuye para cumplir las funciones asignadas. Su competencia genérica es «controlar el procesamiento automatizado de datos personales con riguroso respeto a los derechos humanos y de las libertades y garantías consagrados en la Constitución y en la Ley» (art. 4.1). A la Comisión le corresponde velar por la aplicación del régimen jurídico establecido en la Ley.

La creación y mantenimiento de ficheros, bases o bancos de datos es controlada por la CNPDPI. El régimen de creación de ficheros automatizados se diferencia según contengan datos personales sensibles voluntariamente ofrecidos, o bien, datos personales no sensibles. En el primer caso, debe existir un informe previo de la CNPDPI, tanto si el titular del fichero es un servicio público como si es una entidad privada; en este último supuesto el régimen es de autorización (art. 17.1 en relación con el art. 8.a. y b.). En el segundo caso, es decir, si los ficheros no contienen datos sensibles, la creación debe ser comunicada (art. 17.3).

En la solicitud de informe o autorización, así como en la comunicación dirigida a la CNPDPI, debe declararse la identidad del responsable del fichero; las características del fichero y de su finalidad; los servicios encargados del procesamiento de la información; los datos personales contenidos en el registro; la forma de recogida y actualización de datos; la finalidad a la que se destinan los datos; las entidades a las que pueden ser transmitidos y en qué condiciones; la interconexión de los datos; las medidas de seguridad; el tiempo de conservación de los datos; la categoría de las personas que tienen acceso directo a los datos; la forma y condiciones de ejercicio de los derechos de acceso, rectificación, integración y cancelación (arts. 18 y 19).

El régimen de creación de ficheros fijado por la Ley no es muy claro. En el caso de creación de ficheros de datos personales sensibles se intenta diferenciar dicho régimen según que el responsable del fichero sea una persona pública o privada, ya que se somete a un régimen de informe previo o de autorización, respectivamente. La Ley debería haber creado expresamente un *registro público*, dependiente de la CNPDPI, en el que constase la información sobre los ficheros de bancos existentes, las personas públicas o privadas que los mantienen, siguiendo el modelo de la *Data Lag* sueca de 1973, sometiendo al régimen de autorización e inscripción registral los bancos que

contengan datos sensibles y al de comunicación e inscripción si no son datos sensibles, de modo que la CNPDPI pudiese denegar la inscripción en el registro si el fichero no se somete al régimen legal. El desarrollo reglamentario de la Ley debe completar la garantía institucional mediante la creación del referido registro.

La CNPDPI es titular de potestad reglamentaria. Así, puede emitir directivas para garantizar la seguridad de los datos (art. 8.1.e.); fijar genéricamente las condiciones de acceso a la información, del derecho de rectificación y actualización (art. 8.1.f.). Además, tiene la facultad de proponer su reglamento a la aprobación de la Asamblea (art. 10.3).

La CNPDPI recibe las quejas, reclamaciones y peticiones de los particulares (art. 8.1.h.). Como consecuencia de éstas, puede promover los procedimientos judiciales para interrumpir el procesamiento de datos, impedir el funcionamiento de ficheros y proceder a su destrucción (art. 8.1.g.). Igualmente, debe denunciar al Ministerio Público las infracciones penales (art. 8.1.j.). El desarrollo de estas funciones debe llevar implícita la posibilidad de inspecciones para comprobar si los ficheros comprendidos en el ámbito de aplicación de la Ley se ajustan a su régimen.

La Comisión es un órgano administrativo, y como tal, emite actos administrativos (p. ej., autorizaciones de creación de ficheros, de interconexión de datos) susceptibles de recursos ante el Tribunal Supremo Administrativo (art. 8.2).

Por último, dado que la CNPDPI funciona junto al Parlamento, puede dirigir a la Asamblea sugerencias y recomendaciones relativas al ejercicio de sus competencias. Asimismo, debe dar publicidad a su actividad mediante un informe anual.

B) Delitos y sanciones.

La LPDP tipifica en su capítulo VIII (arts. 34-43) una serie de delitos castigados con penas privativas de libertad[22]. Se tipifica la utilización ilegal de datos (art. 34); la obstrucción al ejercicio de los derechos de acceso, rectificación e integración (art. 35); la interconexión ilegal de ficheros y la atribución de un número de identificación personal (art. 36); el falseamiento de la información de la solicitud de constitución o mantenimiento de ficheros y la omisión de la comunicación de constitución de ficheros que no contengan datos sensibles (art. 38); el acceso ilegal a los datos; la falsificación o destrucción de datos (art. 39); la desobediencia a la orden de interrupción del funcio-

[22] Sobre la protección penal de la libertad informática, *Vid.* F. MORALES PRATS: *La tutela penal de la intimidad: privacy e informática,* Destino. Barcelona, 1884; C. M. ROMEO CASABONA: *Poder informática y seguridad jurídica. La función tutelar del derecho penal ante las nuevas tecnologías de la información,* Fundesco, Madrid, 1988, pp. 25-34. J. BOIX REIG: «Protección jurídico-penal de la intimidad e informática» en en AA.VV., Congreso sobre Derecho Informático. *Texto de Ponencias y Comunicaciones. Edición previa,* 22-24 de junio de 1989, Facultad de Derecho de la Universidad de Zaragoza, pp. 449-492.

namiento de un fichero y la denegación del deber de colaboración (art. 40); y la violación del deber de sigilo (art. 41).

Además de las penas privativas de libertad, se puede imponer como pena accesoria la publicidad de la sentencia en los periódicos, a expensas del condenado (art. 43).

La Ley debería haber tipificado, junto a las infracciones penales, infracciones y sanciones administrativas, así como ilícitos civiles y la correspondiente indemnización de daños y perjuicios. Como señala el art. 10 del Convenio 108 del Consejo de Europa, el régimen de recursos y sanciones debe perseguir que los principios básicos del régimen de protección de datos personales sean respetados.

Reforma de la constitución de Río Negro: necesidad de introducir el tema «Informática y protección de datos personales»

SILVIA C. DE CARTOLANO
Profesora de la Universidad Nacional de Comahué
(ARGENTINA)

INTRODUCCION

El fenómeno informático, esto es la transmisión electrónica de datos a través de un ordenador, ha provocado una revolución tal en la sociedad que, además de calificarla con el término «informatizada» la ha obligado a acelerar la transformación jurídica acorde con el avance tecnológico.

Así como el manejo de la información en forma rápida posibilita una mayor creatividad e implica el cambio de un hombre especulativo actual a un ser «más sociabilizado en el futuro», en razón de disponer mayor tiempo libre; debe considerarse el aspecto negativo de la informática y su impostergable tratamiento y solución por el derecho.

El almacenamiento de «datos personales» y de los llamados «datos sensibles» entendiéndose por tales aquellos que se refieren a la raza, religión, posición política, patrimonio, personalidad psicológica, sexual e historia clínica del individuo, conforman un nuevo concepto de «intimidad» y consecuentemente una actualización del «derecho a la privacidad».

El dato informatizado, para llegar a ser tal, recorre las siguientes etapas: recopilación, procesamiento, introducción en la base de datos, transmisión y difusión. Si bien necesita protección en las distintas etapas, se debe coincidir

que la más delicada es la última, o sea la divulgación, sea interna: entre los organismos del Estado; sea externa: divulgación y manejo con fines distintos de los previstos originariamente.

DERECHO COMPARADO

El Consejo de Europa, organismo internacional creado en Londres el 5 de mayo de 1949, integrado por 21 Estados Democráticos fue el pionero en evaluar el tema de la armonización de la técnica de almacenamiento de datos y la protección de los mismos; habiendo emitido, en los años 73 y 74 recomendaciones en las que se establecen los principios generales a seguir:

–Las informaciones registradas no pueden ser obtenidas por medios fraudulentos o ilícitos.

–Deben ser exactas y actualizadas en forma adecuada y pertinente con respecto a la finalidad que se busca.

–Garantizar que no van a ser utilizadas con finalidad distinta de la prevista.

–Debe conservarse ese archivo de datos hasta que se cumpla con el fin propuesto.

Cuando los bancos de datos procesan «informaciones sensibles», su creación debe estar garantizada por Ley; por una Reglamentación etc; la finalidad de ese Registro debe ser Pública y se deben tomar todas las precauciones necesarias para evitar cualquier abuso o uso indebido de la información.

La persona cuyos datos se almacenan, posee los siguientes derechos: De acceso a los Registros.

–A rectificar la información.

–A ampliar esa información.

–A saber por qué está almacenada esa información y hacia quién va dirigida.

En base a estas dos recomendaciones de carácter general, numerosos Estados Europeos han incorporado a sus Constituciones la Protección de Datos Personales y Sensibles.

Así, la Ley Austriaca del 18 de octubre de 1978, la Constitución Española en su art. 18, la Constitución Portuguesa en su art. 35, La Ley de Libertades francesa de 1978, la Constitución de la República Socialista de Yugoslavia de 1974, en su art. 75 garantiza,el derecho de acceso a la información. En todas ellas se garantiza el derecho a la intimidad en su nueva concepción frente a la existencia de Bancos de Datos Personales.

REPUBLICA ARGENTINA: CONSTITUCIONES PROVINCIALES

Durante los años 1986 y 1987, numerosas constituciones provinciales han considerado la necesidad de una reforma y por ende actualización de los derechos, declaraciones y garantías que le corresponden a las personas.

En relación al tema, la Constitución de Santiago del Estero en su art. 18 establece:

«Todos los habitantes tienen los siguientes derechos conforme a las leyes que reglamenten su ejercicio, a la vida, a la libertad, al honor, a la seguridad, a la intimidad, y a no ser sometido a torturas ni a tratos crueles, inhumanos o degradantes y al nombre.»

«Ningún habitante puede sufrir ingerencias o ataques arbitrarios en su vida privada, su familia, su domicilio, su correspondencia su honra, o su reputación.»

La Constitución de la Provincia de La Rioja, sancionada en 1986, siguiendo los lineamientos establecidos en el art. 18 de la Constitución Española, estatuye en su art. 30:

«Son inviolables el domicilio, los papeles y registros de datos privados, la correspondencia epistolar y las comunicaciones de cualquier índole. Sólo pueden ser allanadas, intervenidas, interceptadas o registradas en virtud de orden escrita de Juez competente.»

«La ley limitará el uso de la Informática para preservar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.»

«El allanamiento de domicilio en horas de la noche es excepcional debiendo el magistrado que lo dispone fundar la decisión.»

«Las autoridades policiales sólo proporcionarán antecedentes penales y judiciales de los habitantes en los casos previstos por la ley.»

La Constitución de San Juan, que rige desde el 1 de mayo de 1986, establece en su art. 26:

«Todo ciudadano tiene derecho a tomar conocimiento de lo que de él conste en forma de registro y de la finalidad a que se destinan las informaciones, pudiendo exigir la rectificación de datos, así como su actualización.»

«No se puede utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se destine para fines estadísticos no identificables.»

La Constitución de San Juan avanza con relación a las anteriores ya que establece derechos de acceso, rectificación y actualización de datos.

La Constitución de la Provincia de Córdoba, sancionada en abril de 1987, en su art. 50 dispone:

«Toda persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información, y a exigir su rectificación y actualización.

Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros excepto cuando tengan un interés legítimo.»

«La ley reglamenta el uso de la Informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.»

Esta Carta profundizó aún más el tema, pues cuando habla de «propósitos discriminatorios de ninguna clase» la exposición de motivos expresa que se debe interpretar esa amplitud a los datos gremiales. Además habla de «personas» en lugar de «ciudadanos» protegiendo a las personas jurídicas y a las entidades de hecho.

Con estos fundamentos la Comisión de Declaración de Derechos y Garantías, por dictamen 023 del 8 de abril de 1988 aconseja a la Convención Constituyente de la Provincia de Río Negro la aprobación del siguiente artículo:

«La ley asegura la intimidad de las personas.»

«El uso de la información de toda índole o categoría almacenada, procesada o distribuida a través de cualquier vínculo físico o electrónico respetará el honor, la privacidad de las personas y el goce completo de sus derechos.»

«La ley reglamentará su utilización de acuerdo a los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguarda de la seguridad, apertura de registro, limitación en el tiempo y control público, asegurando el acceso del sujeto a la información, para la rectificación, actualización y cancelación de la misma, cuando se cumplan sus fines.»

Dicho artículo incorporado a la nueva Constitución en el capítulo referente a Declaraciones, Derechos y Garantías bajo el número 20 es declarativo, siguiendo la tesis brasileña en cuanto a la protección de las personas jurídicas en especial las pequeñas y medianas empresas, habla de personas apartándose de esta forma de la tesis civilista.

BIBLIOGRAFIA

Conferencia sobre «Protección de Datos Personales» ALEXANDER PAPANDREU *1.*[AS] Jornadas de Derecho Informático-UNBA sept. 86.

«La Informática y el Derecho a la Privacidad» VITTORIO FROSSINI Rev. Agora Italia 1983/2 pag. 42.

«Derecho de la Información: Una breve introducción» JON BING Rev. Agora Italia 1983/2 pag. 38.

«Intimidad e Informática en la Constitución» A. E. PÉREZ LUÑO *Edit. Tecnos* – Madrid 1984.

«Informática: Leyes de Protección de Datos(II) Documentación Informática n.º 3 serie verde/Legislación– Servicio Central de Publicaciones –Presidencia de Gobierno de Madrid-1983.

Constitución de España: art. 18 4ta. parte: «La ley limitará el uso de la Informática para garantizar el "honor y la intimidad personal y familiar de los ciudadanos" y el pleno ejercicio de sus derechos».

Constitución de la República de Portugal: art. 35: «Todos los ciudadanos tendrán derecho a tomar conocimiento "de lo que conste en forma de registros mecanografiados acerca de ellos y de la finalidad a que se destinen las informaciones" y podrán exigir la rectificación de los datos, así como su actualización».

Segunda parte: «No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa, o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos».

Tercera parte: «Se prohíbe atribuir un número nacional único a «los ciudadanos».

«Informática y Derecho a la Intimidad, su tutela constitucional» Ricardo Bianciotti-V Congreso Nacional de Informática, Teleinformática y Telecomunicaciones– USUARIA/87 Jun. 87.

«Anteproyecto de Ley de Protección de Datos Personales» Subsecretaría de Ciencia y Técnica-Ministerio de Educación y Justicia –Argentina.

«Datos Personales, Libertad y Derechos Humanos» CARLOS MARÍA CORREA La Razón 24.10.86.

La protección de los datos de carácter personal registrados en soporte informatizado con fines estadísticos, en el Derecho español

MANUEL HEREDERO HIGUERAS
Doctorado en Derecho
Pertenece al Cuerpo Superior de Administradores Civiles del Estado
Experto del Grupo de Relaciones Contractuales de la Confederación de Asociaciones Europeas de Usuarios de Ordenadores (ESPAÑA)

I

El artículo 2-3 del proyecto de LORTAD contiene un cuadro de excepciones a la aplicación de la ley. A diferencia de las excepciones del artículo 2-2, que contemplan lo que podrían calificarse de «sectores exentos», las del artículo 2-3 comprenden sectores en los que ya existen normas de protección de datos, bien equivalentes, en principio, como son los ficheros electorales (apartado a) o los estadísticos (apartado d), bien más intensas, como es el caso de las disposiciones referentes a los datos del Registro Civil, y del Registro Central de Penados y Rebeldes (apartado c). Asimismo, el precepto contempla determinados ámbitos en los que, por incidir en la seguridad del Estado, deben primar el interés de la defensa o la seguridad o el interés público sobre el interés individual, como es el caso de las materias clasificadas (apartado b) o los expedientes del personal militar (apartado e): estas disposiciones no contienen normas protectoras de datos, pero configuran un sistema protector que, en parte, deroga el sistema general de la LORTAD. Si

las disposiciones del apartado c) se considera que van más allá de la LORTAD, las de los apartados b) y e) no alcanzan el nivel de ésta, pero en ellas priman otros intereses.

Las disposiciones referentes a los ficheros electorales y estadísticos se declaran, por ello, subsistentes, debido a que, por configurar un sistema protector especial, constituyen en cada caso lex specialis con respecto a la LORTAD. Según esto, no procedería una aplicación supletoria ni subsidiaria de la LORTAD, ya que se trataría de conjuntos normativos completos, y «sin resquicios». En realidad, no es así por lo que se refiere a las disposiciones de la Ley de la Función Estadística Pública (LFEP), pues el propio artículo 2-3 d) contiene una remisión al artículo 36 m), que da lugar de hecho a que la LORTAD sea aplicable en parte a los ficheros estadísticos, en el aspecto competencial y en lo referente al dispositivo coactivo.

Objeto de este trabajo es analizar las disposiciones que el artículo 2-3 d) deja subsistentes, a saber, las de la ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y la incidencia de la remisión del artículo 36 de la LORTAD. Nada dice el precepto acerca de las leyes de estadística de las Comunidades Autónomas (Canarias, Cantabria, Cataluña, Galicia, País Vasco y Valencia), las cuales contienen asimismo normas protectoras de datos. En este trabajo se contempla el conjunto del ordenamiento positivo en materia de protección de datos registrados con fines exclusivamente estadísticos, por lo cual abarca igualmente el régimen de protección de datos de las Comunidades Autónomas, no siempre coincidente con el de la LFEP ni siempre uniforme[1].

II

La LFEP es una de las primeras leyes de estadística que ha acometido los problemas de la protección de datos. En general, ni las leyes de estadística contemplan estos problemas, ni las leyes de protección de datos se ocupan

---

[1] Las leyes de estadística que se mencionan a lo largo del texto son las siguientes: LFEP (Ley 12/1989, de 9 de mayo, «B.O.E.» de 11 de mayo); ley de Canarias (Ley 1/1991, de 28 de enero, de Estadística de la Comunidad Autónoma de Canarias, «B.O.C.A.» de 11 de febrero); ley de Cantabria (Ley 3/1990, de 21 de marzo, de estadística de Cantabria, «B.O.C.» de 9 de abril); ley de Cataluña (Ley 14/1987, de 9 de julio, de Estadística de la Comunidad Autónoma de Cataluña, «D.O.G.C.» de 27 de julio); ley de Galicia (ley 9/1988, de 19 de julio, de Estadística de Galicia, «D.O.G.» de 3 de agosto); ley del País Vasco (ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi. «B.O.P.V.» de 29 de octubre); Ley de Valencia (Ley 5/1990, de 7 de junio, de Estadística de la Comunidad Valenciana, «D.O.G.V.» de 28 de junio). Estas son las leyes autonómicas de estadística en vigor a 30 de junio de 1992. Las referencias que se hacen al texto del proyecto de LORTAD se entienden hechas al texto del proyecto remitido al Senado por el Congreso de los Diputados, publicado en el «B.O.C.G.» (Senado), Serie II, de 1 de junio de 1992. Por «Convenio 108» debe entenderse el Convenio para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981, ratificado por España y publicado en el «B.O.E.» de 15 de noviembre de 1985.

de los ficheros estadísticos, a excepción de la ley alemana federal de protección de datos de 1990 y la ley danesa de ficheros públicos de 1978/1991. Tampoco existe un texto internacional orientador, al modo de la Recomendación R (87) 15 del Comité de Ministros del Consejo de Europa, sobre el uso de datos personales con fines policiales. La Recomendación R (83) 10, asimismo del Comité de Ministros del Consejo de Europa, no es un texto comparable. Esta Recomendación, aprobada el 23 de septiembre de 1983 [2], no contempla exclusivamente el uso de los datos personales a fines estadísticos, sino que lo encuadra en un marco más amplio que comprende el uso de los datos personales en proyectos de investigación científica, a cuyo efecto considera «investigación» la recogida y proceso de datos personales con fines estadísticos. La Recomendación contiene principios aplicables a ambos contextos, y principios específicos referentes al contexto estadístico. El texto fue redactado antes de que tuvieran lugar las alteraciones del orden público que en los Países Bajos y Alemania Federal originaran las leyes de censos de población de la década de los ochenta [3] y de que, como consecuencia de tales alteraciones, el Tribunal Constitucional Federal alemán dictara la sentencia de 15 de diciembre de 1983 [4]. Sólo a título complementario contiene el texto de la Recomendación principios aplicables a los datos estadísticos. Así, el principio 3.2, que matiza el llamado «principio del consentimiento» con relación al supuesto de la dación voluntaria de datos personales, en el cual el interesado debe ser informado de que es libre de prestar o rehusar su colaboración. El principio del consentimiento se recoge asimismo en el principio 4.1, párrafo segundo, según el cual los datos personales no podrán ser utilizados para adoptar decisiones o medidas que afecten directamente al interesado, sin el consentimiento de éste. En todo caso, el consentimiento es una norma subsidiaria, que sólo se aplica en defecto de mandato imperativo. Puede observarse que el texto corresponde a una etapa del desarrollo doctrinal anterior a la Sentencia del Tribunal Constitucional Federal alemán de 1983, que situaría el problema de los datos estadísticos en el contexto de la licitud de la recogida de los datos personales en general. Es precisamente esta insuficiencia de la Recomendación R (83) 10 en relación con el contexto estadístico lo que ha motivado que el Comité de Expertos de Protección de Datos del

[2] Recomendación R (83) 10 del Comité de Ministros del Consejo de Europa a los Estados miembros, relativa a la protección de los datos de carácter personal utilizados con fines de investigación científica y de estadística, aprobada el 23 de septiembre de 1983, incluida en el volumen Recomendaciones y Resoluciones del Comité de Ministros del Consejo de Europa en Materia Jurídica, Madrid, Centro de Publicaciones del Ministerio de Justicia, 1992, págs. 354-359.

[3] Sobre los antecedentes y vicisitudes de la ley del Censo de Población, Profesiones, Viviendas y Centros de Trabajo (Volkzählungsgesetz 1983), de 25 de marzo de 1982, véase la obra colectiva Die Volkzählung, ed. J. Taeger, Rororo aktuell, Reinbek (Hamburgo), Rowolth Verlag, 1983.

[4] «BVerfG», E 65. Hay versión española, de M. DARANAS, publicada en el «Boletín de Jurisprudencia Constitucional» (BJC), Madrid, Cortes Generales, 1984-33, págs. 126-170.

Consejo de Europa haya acordado el pasado año elaborar una Recomendación específica para los datos estadísticos y los censos de población.

III

a) Tanto la LFEP como las leyes autonómicas de Estadística basan su sistema protector de los datos personales en un concepto amplio de éstos. La LFEP sólo define los datos personales dentro del marco del secreto estadístico (capítulo III del Título Primero). El artículo 13-2 define el concepto de datos personales a esos solos efectos. Por ello, incluye en tal concepto los datos referentes a personas físicas o jurídicas. La misma noción se recoge en los artículos 10-1 y 12-1. Esta acepción amplia del concepto de dato personal es conforme con el espíritu del Convenio 108 del Consejo de Europa, cuyo artículo 3-2 b) faculta a los Estados parte a hacer extensiva la protección a los datos referentes a las personas jurídicas e incluso a las agrupaciones de personas carentes de personalidad jurídica. De las leyes de protección de datos existentes, sólo la noruega (1, párrafo segundo) y la danesa de ficheros públicos (2) extienden la protección a los datos de las personas jurídicas. No así la LORTAD: si en el proyecto del Gobierno se había incluido una disposición final que autorizaba al Gobierno a incluir en el ámbito de aplicación de la ley los ficheros de asociaciones, etc., el texto remitido al Senado no contiene esta autorización reglamentaria. En todo caso, el concepto de dato personal a efectos estadísticos se completa con la exigencia de que el dato permita la identificación inmediata o indirecta de la persona física o jurídica interesada. La identificación indirecta tiene lugar cuando así resulta de la estructura, contenido o grado de agregación: es el caso de la inferencia estadística. Las leyes autonómicas de estadística recogen este concepto amplio, usando la misma dicción que la LFEP, como es el caso de las leyes de Cantabria (artículo 24-1), Cataluña (artículo 26-1), Galicia (artículo 24-1) y Valencia (artículo 20, Uno). Menos claro es el caso de las leyes de Canarias y del País Vasco, que aluden solamente a datos individuales (artículo 19 de la ley de Canarias) y a datos identificables como propios de personas concretas (artículo 20-1 a) de la ley del País Vasco). Sin embargo, el trato de los datos no es el mismo en el caso de las personas físicas y de las jurídicas. Si bien en uno y otro caso la dación es obligatoria, siempre que exista la habilitación legal pertinente, sin embargo la regulación es distinta en lo que respecta al alcance del secreto estadístico. El artículo 16-1 LFEP excluye del secreto los directorios que no contengan más datos que las simples relaciones de establecimientos, empresas, explotaciones u organismos de cualquier clase en cuanto aludan a su denominación, emplazamiento, actividad o intervalo de tamaño.

Esta exclusión no tiene un equivalente en el caso de los datos relativos a personas físicas.

b) La legislación estadística no distingue, a efectos de la protección de los datos, entre los registrados en ficheros manuales y los registrados en soporte informatizado. El artículo 12-2 LFEP prevé la posibilidad de que los datos recabados se den por escrito, en soporte magnético, o de otro modo que permita el ulterior proceso informático. En todo caso, se deja a las normas reguladoras de cada estadística en particular la forma o procedimiento de facilitar los datos. En términos análogos se expresan la ley de Canarias (artículo 16-3), la de Cantabria (artículo 22), la de Cataluña (artículo 27), la de Galicia (artículo 22), la del País Vasco (artículo 12) y la de Valencia (artículo 19). Estas disposiciones son conformes con el artículo 5 de la LORTAD, pues, aun cuando ésta sólo contempla los ficheros informatizados, no limita la recogida de los datos a los procedimientos o soportes informatizados.

IV

La regulación de la protección de datos contenida en la LFEP y en las leyes autonómicas de estadística se centra en la recogida de datos.

a) La primera cuestión que ésta suscita hace referencia a la licitud de la recogida forzosa de los datos estrictamente personales. En principio, toda dación de datos personales debe ser voluntaria, de tal manera que la dación forzosa constituye una limitación del derecho al libre desarrollo de la personalidad. Este derecho, recogido de un modo u otro en las constituciones actuales, tiene como corolario este derecho a decidir sobre la dación de tales datos. Es el derecho de autodeterminación sobre la información personal, definido en 1983 por el Tribunal Constitucional Federal alemán per modum determinationis a partir del derecho al libre desarrollo de la personalidad, que la Ley Fundamental de Bonn reconoce en su artículo 2-1. El reconocimiento de este derecho trae consigo la necesidad de una habilitación legal para poder obligar a las personas a que den datos sobre sus circunstancias personales. Por consiguiente, la recogida de tales datos requiere una habilitación expresa por vía de norma de rango legal que, además, sea conforme a la constitución (verfaungsmssig). La CE no contiene, a diferencia de la Ley Fundamental de Bonn, una formulación genérica de un derecho al libre desarrollo de la personalidad, aun cuando tal derecho está presente en diversos perceptos constitucionales, como los artículos 14, 15, 16, 18, 19, 20-1 b), 27-2, 38, 44-1, por ejemplo. La LFEP recoge esta doctrina. En su preámbulo se invocan los artículos 18-1 y 53-1 CE, como base de la exigencia de la habilitación legal para la recogida forzosa de los datos con fines estadísticos. Asimismo hace hincapié en el preámbulo en el carácter esencial que al respecto ofrece la recogida de los datos. Por ello, la ley dedica a este problema los artículos 4 a 12. En estos preceptos no se hace distinción entre datos personales y no personales. El primero define los principios de secreto, transparencia, especialidad y proporcionalidad, como criterios a los cuales debe ajustarse la

recogida de datos. Estos principios se definen en los apartados 2 a 4 del artículo 4. El principio de secreto se concreta en la exigencia de adoptar medidas organizativas y técnicas para proteger la información, como medio de garantizar el secreto estadístico, regulado en el Capítulo III. En realidad, este principio no hace sino transponer la norma del artículo 7 del Convenio 108, recogida, a su vez, en el artículo 9 de la LORTAD. El principio de transparencia implica la exigencia de informar a las personas que deben suministrar los datos acerca de la protección de los datos recabados y de la finalidad a que se destinan. El principio de especialidad, según se define en el artículo 4-4, concuerda con el que la doctrina denomina «principio del uso racional de los datos»: en su virtud, «es exigible a los servicios estadísticos que los datos recogidos para la elaboración de estadísticas se destinen a los fines que justificaron la obtención de los mismos». Por último, el principio de proporcionalidad consiste en la correspondencia entre la cantidad de la información que se solicita y los resultados que de su tratamiento se pretenden obtener. Estos principios transponen los que se definen en el artículo 5 del Convenio 108 del Consejo de Europa. La LFEP los hace extensivos a los datos no estrictamente personales, en la medida en que, como quedó dicho, no hace distinción entre unos y otros. La LFEP exige en su artículo 7-1 que se establezcan por ley las estadísticas para cuya elaboración se exijan datos con carácter obligatorio. El artículo 7-2 prevé un contenido mínimo para estas leyes: organismos que deben intervenir en su elaboración, enunciado de sus fines y descripción general de su contenido, colectivo de personas, ámbito territorial de referencia, y créditos presupuestarios para su financiación. La disposición adicional cuarta de la Ley 4/1990, de 29 de junio, de Presupuestos Generales del Estado para 1990, contiene una primera habilitación a tal efecto, que cumple con los requisitos del artículo 7-2. Distinta es la cuestión de si el cauce de una ley de Presupuestos es el idóneo. Exista o no esta habilitación legal para la recogida forzosa de datos, el artículo 11-2 LFEP, exige, en todo caso, el consentimiento expreso del interesado cuando se trata de recabar datos capaces de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas y, en general, cuantas circunstancias puedan afectar a la intimidad personal o familiar. Este precepto transpone la norma del artículo 16-2 de la CE, según el cual nadie puede ser obligado a declarar sobre sus opiniones políticas o convicciones religiosas o ideológicas. Hay que admitir, por tanto, que la habilitación para la recogida de datos, contenida en el artículo 7-2 de la LFEP y normas de desarrollo se sitúa en el rango normativo pertinente. Cabe incluso admitir que el nivel de protección de los datos personales, previsto en la LFEP, es superior al de la LORTAD, pues, si se compara el artículo 7-1 de la LFEP con los artículos 4 y 6 de la LORTAD, estos últimos configuran un sistema protector menos intenso, debido a que no exigen en todo caso la habilitación legal ni el consentimiento del interesado para la recogida de los datos. La exigencia del consentimiento se limita, por otra parte, a la recogida. La LFEP no contiene

una norma análoga a la del artículo 11 de la LORTAD, que prevé el consentimiento del interesado como condición para la cesión de sus datos. Sólo la ley de Canarias (artículo 23) reconoce al interesado un derecho a renunciar al secreto estadístico, mediante una declaración por la que consienta la cesión de sus datos.

b) Estos principios de la recogida de datos no figuran en las leyes autonómicas de estadística. En dichas leyes se enuncian unos principios, que se basan en una consideración de las técnicas estadísticas desde otro ángulo. Unicamente los que se denominan principio de la obligación de colaboración ciudadana y respeto a la intimidad hacen referencia a la recogida de datos. Los demás, como los de interés público, objetividad y corrección técnica, y publicidad de los resultados, inciden en el proceso estadístico propiamente tal, que se desarrolla en un momento ulterior. Las leyes autonómicas recogen los dos primeros, casi con la misma formulación. El principio de la colaboración ciudadana se recoge en las leyes de Canarias (artículo 14), Cantabria (artículo 18), Cataluña (artículos 25 a 27), Galicia (artículo 18), País Vasco (artículo 10) y Valencia (artículo 14, Uno). Si consideramos, desde otro ángulo, que la dación obligatoria de los datos personales constituye una prestación personal obligatoria, que, en cuanto restricción de la libertad, requiere una habilitación legal conforme a la constitución, hay que admitir que el principio de la obligación de colaboración ciudadana tiene también un apoyo en la CE, en el artículo 31-3, que exige el cauce de la ley para imponer prestaciones personales. La consideración de la dación de datos como una prestación obligatoria tiene además otra justificación, que es la de servir de fundamento al derecho al resarcimiento de los gastos irrogados por la dación de los datos. Esta contrapartida está presente en la LFEP (artículo 12-3) y en las leyes de Canarias (artículo 16-3), Cantabria (artículo 23), Cataluña (artículo 29), Galicia (artículo 23) y Valencia (artículo 19).

c) Aun en el supuesto de que exista la habilitación de una norma de rango legal que permita obligar a dar los datos, la recogida tiene unos límites, que vienen impuestos por preceptos constitucionales. La LFEP concuerda con la LORTAD, en la medida en que el artículo 11-2 transpone avant la lettre la norma del artículo 7 de la LORTAD. El artículo 11-2 de la LFEP dispone que son, en todo caso, de aportación estrictamente voluntaria y que, por tanto, sólo pueden recogerse previo el consentimiento expreso del interesado, los datos «susceptibles de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas» y, en general, cuantas circunstancias puedan afectar a la intimidad personal o familiar. Este precepto reúne en un mismo conjunto los datos personales que, según el artículo 16-2 de la CE sólo pueden ser dados voluntariamente –ideología, religión y creencias–, y además los datos que revelen el origen étnico y cuantas circunstancias puedan afectar a la intimidad personal o familiar. Habrá que entender que esta última expresión cubre aquellas circunstancias que, por su naturaleza

y dentro de las normas morales o sociales imperantes en el colectivo de que se trate, deban ser tratadas con cautela, en la medida en que su registro en soporte manual o informático cree riesgos para la reputación del interesado. Así, una encuesta que tuviera por objeto la situación familiar, filiación, vida sexual, historia clínica, etc. sólo podría hacerse con el previo consentimiento del interesado. En todo caso, no es fácil determinar el alcance de la limitación que para la recogida de datos con fines estadísticos imponen algunas de las leyes de estadística en aras del «derecho al honor». Circunstancias personales cuyo conocimiento y difusión habría contribuido a menoscabar el respeto o la estimación de una persona, a su desprestigio o mala reputación, han perdido todo significado a tal efecto. Así, la filiación ilegítima, la homosexualidad, la conducta de los parientes, etc. tenían una influencia dentro de un contexto social que no es el actual. El concepto se diluye aún más en el caso de las personas jurídicas –cuyos datos están asimismo protegidos por la legislación de estadística. ¿Podrá negarse una empresa a contestar un cuestionario de recogida de datos que contenga preguntas atentatorias contra la fama o prestigio de la empresa? ¿Cuáles pueden ser tales preguntas? [5].

d) Esta limitación de la recogida de datos figura, con algunas variantes, en las leyes de estadística de las Comunidades Autónomas. El artículo 21-1 de la ley de Canarias, no obstante su sedes materiae (la sección tercera del Capítulo Primero del Título II, dedicado al secreto estadístico), se aplica a la totalidad de la actividad estadística regulada por la ley, por lo cual hay que entender que la recogida de los datos personales tiene su límite en los artículos 16-2 y 18-4 de la CE. El artículo 20 de la ley de Cantabria prohibe que los cuestionarios contengan preguntas que guarden una relación directa con el derecho al honor, a la intimidad personal y familiar y las convicciones religiosas o políticas del informante (artículos 16-2 y 18 de la CE). La misma norma figura en el artículo 20 de la ley de Galicia y en el artículo 18 de la de Valencia. Una norma parecida se recoge en el artículo 10 de la ley del País Vasco. Con leves variantes se recoge también esta norma en el artículo 28 de la ley de Cataluña. Según este precepto, los cuestionarios respetarán, en todo caso, lo dispuesto en el artículo 18 de la CE – esta remisión al conjunto del artículo 18 puede interpretarse en el sentido de que no sería lícito recoger datos cuando la recogida implicara un allanamiento de morada o una violación del secreto de las comunicaciones que se plasmara en el registro informatizado o manual de una información obtenida por medio de una escucha telefónica. Asimismo, prohíbe que los cuestionarios contengan preguntas que tengan una relación directa o indirecta con el honor personal o con las convicciones religiosas o políticas del informante. El precepto exceptúa los casos en los que por la forma en que se recoja la información, ésta no pueda ser atribuida a una persona determinada, a menos que, habiendo

[5] Cfr. FELIU REY, M. I., ¿Tienen honor las personas jurídicas?, Madrid, Tecnos, Colección Jurisprudencia Práctica, 1991.

sido solicitada la información de la forma adecuada, el propio interesado diera lugar a la singularización, por su negativa o retraso en darla.

e) Otros principios de la recogida de datos, aun cuando no se denominen principios ni se consideren formalmente como tales, son los que se expresan en los artículos 11-1 y 12-1 LFEP. El primero exige que a los interesados se les informe suficientemente sobre la naturaleza, características y finalidad de la estadística, advirtiéndoseles, además, de si es o no obligatoria la colaboración, de la protección del secreto estadístico y de las sanciones en que pudieran incurrir por no colaborar o por dar datos falsos, inexactos, incompletos o extemporáneos. El segundo recoge la norma de que los datos deben solicitarse directamente de los interesados. Estos principios se recogen asimismo en las leyes de Estadística de las Comunidades Autónomas. El primero figura en las de Canarias (artículo 17), Cantabria (artículo 19-1), Galicia (artículo 19-1) y Valencia (artículo 17). El segundo sólo figura en las del País Vasco (artículo 11) y Cataluña (artículo 5-2).

f) La norma de la recogida directa de los datos no impide que puedan asimismo recabarse indirectamente, en la medida en que, a tenor de las disposiciones pertinentes de las leyes de estadística, los organismos públicos estén obligados a dar sus datos, según resulta de los artículos 10-3 y 10-4 de la LFEP y de los preceptos concordantes de las legislaciones autonómicas (Canarias, artículo 15-3; Cantabria, artículo 21-2; Cataluña, artículo 11; Galicia, artículo 21-2; País Vasco, artículo 10-3). Esta cesión obligatoria de los datos por parte de los órganos y organismos de las Administraciones públicas se recoge en algunas leyes autonómicas, a través de la distinción entre datos estadísticos y datos administrativos, que figura en las leyes de Canarias (artículo 34-1) y País Vasco (artículo 5-2). Los segundos son los datos obtenidos de la gestión administrativa o de operaciones específicas de recogida de información para uso administrativo. Esta norma de la recogida indirecta o cesión obligatoria no es conforme con el principio del consentimiento, al menos en la formulación que del mismo contiene el artículo 11-1 de la LORTAD. En todo caso, una vez que ésta hubiere entrado en vigor, el interesado tendrá siempre derecho a que se le informe de los fines y usos de los datos que le recabaren las Administraciones públicas, a tenor del artículo 5 de la LORTAD. De este modo, la LORTAD completará el cuadro protector de la LFEP y de las leyes autonómicas de estadística.

V

Una vez recogidos los datos lícitamente para fines estadísticos, surgen otros problemas de protección de datos, que hacen referencia al uso de los datos recogidos, tales como la adecuación de dicho uso con los fines de la recogida, la conservación de los datos en función de tales fines, su cesión, y el secreto de los datos.

a) Ante todo, los datos no podrán ser utilizados para otros fines. Es lo que el artículo 4-4 de la LFEP, denomina principio de especialidad, que concuerda con el que expresa el artículo 5, apartado b) del Convenio 108. Entre los fines ilícitos debe incluirse el uso de los datos así recogidos, para adoptar decisiones o medidas que afecten directamente al interesado, excepto con su consentimiento expreso, según el principio 4.1, párrafo segundo, de la Recomendación R (83) 10 del Consejo de Europa. En términos no del todo coincidentes se expresan los artículos 22-3 y 23 de la ley de Canarias. Ambos preceptos, que se encuadran sistemáticamente en la sección referente al secreto estadístico, recogen este principio. El artículo 22-3 sólo permite transmitir (ceder) datos «para la exclusiva finalidad de actividad estadística»; el artículo 23 permite que el interesado renuncie mediante manifestación expresa y por escrito al secreto estadístico, bien con carácter general o para unos usos determinados, en cuyo caso el secreto subsistirá para los demás usos. El principio se recoge en forma más terminante en el artículo 24-3 de la ley de Cantabria, que, en aras del secreto estadístico, prohibe usar los datos estadísticos para finalidades fiscales o policiales, y para cualquier otra finalidad distinta de aquélla para la cual hubieran sido solicitados.

b) El artículo 5, apartado e), del Convenio 108 consagra el principio de la conservación limitada de los datos personales registrados. El precepto precisa que la conservación de los datos, al menos en forma tal que permitan la identificación, debe limitarse al tiempo que fuere necesario en función de las finalidades para las cuales hubieran sido recogidos los datos. Este principio reviste una fisionomía específica en la legislación estadística. En otros ficheros, la información de origen no se conserva, sino que se registra en ficheros informatizados, que son los que se utilizan. En los ficheros estadísticos la peculiaridad estriba en que la información de origen se conserva, bien en el soporte original, bien en soporte informatizado, y que, además, se conserva en forma despersonalizada. La LFEP (artículos 22-2 y 22-3) dispone que la información original podrá destruirse una vez que, a juicio de los servicios estadísticos, su conservación resultare evidentemente innecesaria. No siempre será este el caso cuando exista la posibilidad de facilitar tabulaciones o elaboraciones estadísticas distintas de los resultados hechos públicos (artículo 21-1 a). Estas tabulaciones o elaboraciones podrán hacerse a partir de datos despersonalizados, pero a veces requerirán acudir a la información original. Esta norma de la LFEP sólo tiene una correspondencia en el artículo 16-3 de la ley del País Vasco.

c) La cesión de los datos personales recogidos y registrados con fines estadísticos se regula en las leyes de estadística dentro del cuadro normativo del secreto estadístico. El artículo 13-3 LFEP define el secreto estadístico como la obligación de «no difundir en ningún caso los datos personales, cualquiera que sea su origen». El artículo 15 prevé, sin embargo, excepciones a esta obligación, que no hacen sino transponer el principio que inspira el

artículo 11-1 de la LORTAD, según el cual debe existir una relación biunívoca entre los fines del cedente y los del cesionario. En el caso de los datos estadísticos sólo existe esa relación biunívoca si los datos se los ceden entre sí los servicios estadísticos. El artículo 15-1 LFEP, exige que exista esta correspondencia al disponer que, para que puedan cederse los datos, los servicios que reciban los datos desarrollen funciones fundamentalmente estadísticas y hayan sido regulados como tales antes de que los datos sean cedidos. El destino de los datos debe ser precisamente la elaboración de las estadísticas que dichos servicios tengan encomendadas. Por último, los servicios destinatarios deben disponer de los medios necesarios para preservar el secreto estadístico. Esta última condición es una modulación más de la norma del artículo 7 del Convenio 108, que se une a la del artículo 4-2 LFEP. La norma del artículo 15-1 LFEP tiene un equivalente en las leyes autonómicas de estadística: ley de Canarias (artículo 18), ley de Cantabria (artículo 24), ley de Cataluña (artículo 30), ley de Galicia (artículo 24), ley del País Vasco (artículo 19), ley de Valencia (artículos 20 a 22).

d) El secreto estadístico se recoge pormenorizadamente en todas las leyes estadísticas. Tanto la LFEP como las distintas leyes autonómicas contienen un cuadro normativo preciso para el secreto estadístico: objeto, sujeto, contenido, duración y excepciones. Una vez que entrare en vigor la LORTAD, el secreto estadístico vendrá a constituir una mera norma de transposición de la LORTAD, en la medida en que ésta eleva a norma general lo que en la vieja ley de estadística de 1945 constituyera una innovación, que sería recogida en la LFEP y en las leyes autonómicas. La única diferencia que ofrecen estas últimas con respecto a la LORTAD consiste en el objeto del secreto, pues, en tanto que ésta lo limita a los datos personales –según se definen en el artículo 3–, las leyes de estadística lo hacen extensivo a los datos de las personas jurídicas, empresas, sociedades, etc. El secreto estadístico desborda, por ello, el ámbito de la mera protección de los datos personales y del derecho de autodeterminación individual, en la medida en que con el mismo se protegen intereses comerciales, secretos industriales, y otros bienes análogos, ajenos al derecho a la personalidad. Por lo demás, las leyes de estadística de las Comunidades Autónomas concuerdan con la LORTAD en cuanto a la duración del deber de secreto, que subsiste aun después de extinguida la relación laboral o de servicio (artículo 10 LORTAD; artículo 17-4 LFEP; artículo 22-1 de la ley de Canarias; artículo 26-1 de la ley de Cantabria; artículo 26-1 de la ley de Galicia; artículo 21 de la ley de Valencia).

VI

Los derechos de acceso y rectificación, derechos irrenunciables del interesado o afectado, se encuadran en las leyes de estadística en el marco de la regulación del secreto estadístico. Este encuadre de dichos derechos les con-

fiere un sesgo especial. El artículo 16-4 L.F.E.P. reconoce un derecho de acceso del interesado a sus datos, pero sólo con ciertas limitaciones:

«los interesados tendrán derecho de acceso a los datos personales que figuren en los directorios estadísticos no amparados por el secreto estadístico y a obtener la rectificación de los errores que contengan»

El interesado no puede, por tanto, acceder a sus propios datos. El secreto estadístico impide, no sólo que terceras personas accedan a datos de los interesados, sino, además, que el propio interesado los conozca [6]. Esta norma es claramente contraria a las de los artículos 13 y 14 de la LORTAD, que proclaman con carácter general el derecho de acceso, en sentido amplio (artículo 13) y en sentido estricto (artículo 14). En apoyo de esta restricción del derecho de acceso cabría invocar el principio 6.1 de la Recomendación R (83) 10 del Consejo de Europa, que permite limitar el derecho del interesado a obtener y rectificar los datos que le conciernen, cuando los datos se recogen y retienen con fines puramente estadísticos, pero siempre que las estadísticas «no permitan identificar fácilmente a la persona». Este principio tiene su base en la norma del artículo 9-3 del Convenio 108, que autoriza excepciones al régimen general de la protección de los datos precisamente en materia estadística. Sin embargo, la memoria explicativa de la Recomendación (apartado 39) matiza que esta excepción sólo procede cuando los datos se usan en forma no identificable, es decir, cuando los datos han sido previamente despersonalizados. En tales casos lo que sucede, en realidad, es que el acceso a los datos resulta imposible. Habrá que admitir que, siempre que los datos no estén despersonalizados, debería permitirse el acceso y, en consecuencia, la rectificación de los datos que, en su caso, fueran erróneos. Esta interpretación concuerda asimismo con la norma del artículo 21-1 a) LFEP, que permite que los servicios estadísticos faciliten a quien lo solicite, datos individuales que no estén amparados por el secreto estadístico «porque hayan llegado a ser anónimos hasta tal punto que sea imposible identificar a las unidades informantes».

En las leyes autonómicas la regulación del derecho de acceso a los datos personales varía según la Comunidad Autónoma de que se trate. La ley de Canarias reconoce en su artículo 20-3 los derechos de acceso y rectificación, sin las limitaciones del artículo 16-4 LFEP:

«Los interesados tendrán derecho de acceso a los datos personales que les conciernan, que figuren en los directorios estadísticos y a obtener, en su caso, la rectificación de los errores que contuvieren.»

En cambio, la ley de Cantabria, en su artículo 27-3, sólo admite el derecho de acceso como una excepción al secreto estadístico. Siempre que hubie-

[6] Cfr. Informe del Defensor del Pueblo correspondiente a la gestión realizada durante el año 1991, «B.O.C.G.» (Sección Cortes Generales), IV Legislatura, Serie A: Actividades Parlamentarias, 25 de abril de 1992, núm. 37, págs. 62 a 68.

ran transcurrido, al menos, veinticinco años desde la recogida de la información, podrán facilitarse datos protegidos por el secreto estadístico a quien acredite un legítimo interés, y ello por el cauce del procedimiento que se establezca reglamentariamente. Cabe entender que ese interés legítimo asiste al afectado o titular de los datos. Una norma parecida se recoge en el artículo 27-2 de la ley de Galicia. Sólo varía el plazo, que, en general, para la observancia del secreto estadístico es de 100 años y de 60 excepcionalmente para facilitar datos a quien acredite un interés legítimo, a efectos de análisis histórico, y pretenda publicar los resultados de los análisis. En iguales términos se expresan el artículo 21 de la ley del País Vasco y el 26 de la ley de Valencia. Esta regulación es aún más limitada que la de la ley de Cantabria, puesto que la condición del interés legítimo debe ir unida a que el acceso se haga a efectos de análisis histórico.

VII

a) La remisión que el artículo 2-3 d) del proyecto de LORTAD hace a las disposiciones específicas de la LFEP. Se refiere, en rigor, a las que regulan el proceso de recogida de datos y al ulterior uso de los datos. En cambio, el control de la aplicación de las disposiciones de protección de datos de la LFEP no corresponde al Instituto Nacional de Estadística, sino que se encomienda a la Agencia de Protección de Datos. Para ello, el citado artículo 2-3 d), in fine, se remite al artículo 36, apartado m), de la LORTAD, que expresamente atribuye tal competencia a la Agencia. En consecuencia, las operaciones de recogida de datos, tales como la concepción y redacción de los cuestionarios, la interrelación de los ficheros estadísticos, con miras o no a operaciones de inferencia estadística, y demás aspectos específicamente relacionados con la protección de los datos personales, requerirán el dictamen o la intervención de la Agencia de Protección de Datos, pero siempre dentro del marco de las disposiciones de la LFEP. La Agencia de Protección de Datos no aplicará, por tanto, las disposiciones de la LORTAD en el contexto estadístico. Unicamente en materia disciplinaria, como resulta del artículo 36 m), in fine, aplicará la Agencia lo dispuesto en el artículo 43 de la LORTAD, que regula las infracciones en materia de protección de datos y, en consecuencia, las medidas extraordinarias que en tal contexto prevé el artículo 45 de la LORTAD. Las infracciones y sanciones previstas en los artículos 48 y 50 a 54 LFEP sólo serán aplicables en la medida en que no se refieran a los supuestos de hecho tipificados y sancionados en los artículos 43 y 44 de la LORTAD. El Instituto Nacional de Estadística se configura así como un «responsable de ficheros», concretamente de los ficheros estadísticos estatales, sujeto a la tutela funcional de la Agencia de Protección de Datos.

b) Limitada la competencia de la Agencia de Protección de Datos al control de la aplicación de la LFEP, surge el problema del alcance de lo dispuesto en el artículo 40 de la LORTAD en lo que respecta a los ficheros

estadísticos creados o gestionados por las Comunidades Autónomas. Excepto las funciones de la Agencia que consisten en la publicidad de la existencia de los ficheros automatizados de datos de carácter personal, la elevación de una Memoria anual al Ministro de Justicia, y la policía de las transferencias internacionales de datos, todas las competencias de la Agencia, incluso la llevanza de registros propios de ficheros informatizados públicos, pueden ser asumidas por los órganos correspondientes de cada Comunidad. Los ficheros estadísticos de las Comunidades Autónomas entran claramente en este supuesto. Dado el carácter meramente habilitante de esta norma, caben varias posibilidades: 1) que la Comunidad Autónoma respectiva solicite caso por caso la intervención de la Agencia por vía de dictamen, referido, por ejemplo, a los cuestionarios de recogida de datos o a otras actuaciones del órgano autonómico de estadística, pero sin asumir competencias al respecto; 2) que la Comunidad Autónoma atribuya a dicho órgano autonómico las funciones de la Agencia; 3) que cada Comunidad Autónoma atribuya una función de control de órgano de estadística autonómico a una Agencia de Protección de Datos propia o al órgano que en la Comunidad corresponda al Defensor del Pueblo (Justicia, Ararteko, Síndic de Greuges, etc.); o finalmente, 4) que la Comunidad Autónoma cree un órgano específico de control del órgano autonómico de estadística. Esta última solución ha sido ya adoptada para los ficheros de la policía vasca, por la reciente ley de Policía del País Vasco, que atribuye el control de estos ficheros a una Comisión del Parlamento Vasco. La LORTAD prevé, en todo caso, en el artículo 40-3, un cauce de coordinación y unificación de criterios.

VIII

A modo de conclusiones de este análisis de las disposiciones de protección de datos de la LFEP y de las leyes autonómicas de estadística, cabe señalar lo siguiente: a) la remisión del artículo 2-3 d) del proyecto de LORTAD a las disposiciones de la LFEP sólo es válida en lo que se refiere a las disposiciones sustantivas, pero no en lo relativo al control de la aplicación de la propia LFEP; b) el nivel de protección de datos de las leyes de estadística es adecuado y conforme a la LORTAD en lo que respecta a los principios de la recogida y uso de los datos; c) el nivel protector es, sin embargo, inferior al de la LORTAD por lo que se refiere a las garantías de derecho de acceso y rectificación.

La protección de datos informáticos en el derecho comparado

JOSÉ IGNACIO MARTÍN ONCINA

Abogado
Funcionario de la Admón. Civil del Estado
(ESPAÑA)

I. DERECHO COMPARADO

Por pertenecer España a la Comunidad Económica Europea y estar en íntima relación con los países líderes de la Economía de Mercado, donde tiene un amplio uso la informática para constituir bancos de datos con el más diverso uso, es necesario en un principio, tomar la referencia de la legislación de dichos países. Nos obliga a ello, el vacío legal existente en nuestro pais. Por tanto, habrá que calificar o tipificar los malos usos con el fin de amparar la intimidad reconocida en el artículo 18.4º de la Constitución.

El citado artículo de la Constitución española emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de sus ciudadanos y el legítimo ejercicio de sus derechos.

El progresivo desarrollo de las técnicas de recogida y almacenamiento de datos, así como el acceso a los mismos, ha expuesto la privaticidad a una amenaza potencial antes desconocida.

A falta de Derecho positivo en España, vamos a ver la legislación vigente en los países de nuestro entorno más desarrollados.

ALEMANIA

Los alemanes aman con especial fervor todo cuanto suene a dato informático o ficha. Los archivos cobran dimensiones absurdas. Así, los ciudadanos para abrir una cuenta corriente han de pasar por la Comisaría para declarar cualquier cambio de domicilio.

El Parlamento Alemán aprobó en Junio de 1991 la Ley de Protección de Datos, cuyo fin es salvaguardar los datos almacenados y los actos manuscritos.

Dicha ley se refiere tanto a la utilización pública como a la privada de los datos personales y contempla los puntos siguientes:

1. Protege todo tipo de datos, tanto lo almacenado electrónicamente como las actas manuscritas. Esta última referencia se dirige contra la manipulación de los servicios secretos de la antigua R.D. Alemana.

2. Los datos sobre personas físicas, solamente se podrán utilizar para los fines que fueron requeridos.

3. Si a causa del trabajo automatizado de los datos personales se producen daños, un organismo público puede imponer multas de hasta 15 millones de pesetas, con independencia de las indemnizaciones a las que el sujeto tenga derecho y de las responsabilidades penales que hubiera lugar.

4. Se contempla otro modo de protección de datos, no sólo prohibiendo la diseminación de datos de forma incontrolada, sino haciendo más difícil su utilización. Esto se refleja en la codificación del ordenador, pues sin clave adecuada es imposible usarlos. A ello se debe que existan muchos especialistas en el mundo en descifrar códigos.

Alemania extrema la guarda del secreto de datos informáticos de tipo personal ante la avidez de información de la administración pública y privada.

El Tribunal Constitucional Alemán ha resuelto con la Ley del Censo de 11/12/83, con una prudencia que bien podía ser modelo para el planteamiento en nuestro país del mismo problema. El Alto Tribunal entiende la libertad personal como autodeterminación individual, la cual incluye la autodeterminación informativa. Las personas tienen derecho a decidir por sí mismas cuando y dentro de qué límites procede revelar datos referentes a su propia vida. Facultad esta, necesitada hoy de especial protección, por la injerencia de la informática en la vida individual.

ITALIA

Tiene una Ley que regula el acceso de las personas privadas a la información de la Administración.

Se garantiza a los interesados la visión de datos relativos a procedimientos administrativos, cuyo conocimiento sea necesario para defender intereses

jurídicos de terceros. Si no se da esta circunstancia se podrá negar el acceso a los documentos para salvaguardar la privaticidad.

El Gobierno decide a qué documentos se puede acceder y establece para los funcionarios el deber de guardar el secreto oficial.

La Ley al establecer para todo ciudadano el derecho a acceder a la información, regula también el modo de ejercer este derecho. Así, según su artículo 24 se podrá negar el acceso a los documentos por necesidad de salvaguardar «la privaticidad de terceros, personas o cosas y se puede prohibir el acceso a textos relativos a la seguridad, defensa nacional, relaciones internacionales o por política monetaria».

La Ley encarga a una Comisión regular los casos en que se podrá acceder a la Administración para salvaguardar los intereses de una persona privada. Y los funcionarios no podrán transmitir información ni operaciones administrativas a quien no tenga derecho a ello.

El Estado se reserva fijar a qué documentos puede o no puede acceder el ciudadano en función de los intereses nacionales y de imponer a los funcionarios el secreto profesional en los asuntos que tenga conocimiento por razón de su cargo.

GRAN BRETAÑA

La Ley de Protección de Datos de 1987 vino a salvaguardar la intimidad de las personas que pudieran ser dañadas por el uso o manipulación de datos personales que obrasen en poder de sistemas informáticos oficiales.

Se propusieron tres delitos:

1. Transgresión elemental.– Para el acceso sin autorización a los contenidos y procesos de una computadora.

2. Transgresión grave.– En los casos que se busca el acceso a un sistema informático con el propósito de de cometer o ayudar a cometer un delito. Se castiga con pena privativa de libertad de hasta cinco años.

3. Transgresión más grave.– Cuando se alteran intencionadamente los programas informáticos. Penas privativas de libertad superiores a cinco años.

La Ley de Derechos de autor de 1985 apunta alguna protección respecto al uso sin autorización de discos o cintas de computadora, pero hay que demostrar la existencia del «copyright». Esta ley requiere la prueba de daño causado, puesto que ello ha de constituir la prueba ante los Tribunales para la valoración de daños y perjuicios.

FRANCIA

Los ciudadanos franceses están protegidos desde 1978 contra el abuso o comercio de datos personales informatizados por una Comisión Nacional

para la Informática y las Libertades (CNIL). A ella deben someter sus ficheros todas las entidades y empresas. Todas las empresas, instituciones públicas o privadas que tengan algún tipo de fichero informatizado deben comunicarlo previamente a la Comisión, que a su vez tiene derecho a limitar algunos aspectos de su funcionamiento o manipulación de las informaciones contenidas en el fichero.

La Comisión está integrada por diecisiete miembros nombrados por el Gobierno, el Senado y la Asamblea Nacional.

La legislación existente es particularmente estricta y sólo la Seguridad Nacional puede lograr excepciones a la generalidad.

La Comisión Nacional de la Informática y las Libertades (CNIL), fue una de las primeras instituciones político-jurídicas creada tras la publicación de un célebre estudio realizado por PIERRE NORA y ALAIN MINE, sobre los efectos potencialmente revolucionarios socialmente de la informática en la vida cotidiana de las sociedades industriales avanzadas.

La Administración Pública y el Gobierno están igualmente obligados a someterse a la Jurisdicción de la Comisión Nacional para la Informática y las Libertades.

Solamente el Consejo de Estado y de forma excepcional, alegando razones de seguridad nacional puede eximir del control estricto de la Comisión a la Administración Pública.

La Policía y el Ejército están exentos del control de la Comisión Nacional de la Informática y de las Libertades, pues los problemas de seguridad y orden público deben escapar al control de la Comisión.

Las personas están particularmente protegidas por medio de la CNIL, que prevé para cada ciudadano el derecho a conocer el contenido de los ficheros informáticos donde figure su nombre, el control de las informaciones que le conciernen y su eventual verificación o manipulación.

Las informaciones que pudieran considerarse sensibles, como las opiniones políticas, filosóficas o religiosas no pueden introducirse en un archivo informático sin el acuerdo escrito de las personas afectadas.

Esta Comisión Nacional para la Informática y las Libertades ha evitado cualquier tipo de escándalo en materia de manipulación o comercialización de datos informatizados.

ESTADOS UNIDOS

Sólo existe una jurispruedencia de sentencias motivadas por denuncias de particulares. Esta jurisprudencia es la que crea protección, pero no existe una ley que de forma concreta y específica regule esta materia. La jurisprudencia que es la que se aplica como protección requiere permiso para utilizar datos personales.

El uso fraudulento de datos informáticos personalizados adquiere en EE.UU. dimensiones gigantescas.

Las empresas venden información, adquirida en gran medida a través de las tarjetas de crédito. Así, el comprador de estos datos puede obtener: nombres y direcciones de personas con un determinado nivel económico, tipo de hoteles que utilizan, tipo de tiendas en donde hacen sus compras, nivel de gasto anual, etc.., buscando así sus clientes «tipo».

No existe ninguna legislación federal sobre el uso de los datos informáticos.

PORTUGAL

El artículo 35 de la Constitución portuguesa prohíbe el acceso de terceros a los bancos de datos.

Este artículo autoriza a los ciudadanos a conocer sus datos personales que existan en los ficheros y a ser informados de la utilización que de estos se haga.

El citado artículo 35 de la Constitución establece que la informática no puede ser utilizada en función de las convicciones políticas, filosóficas religiosas, de afiliaciones sindicales, salvo para estadísticas.

No existe Ley que desarrolle de forma concreta el uso de la informática según prevé el artículo 35 de la Constitución.

El uso ilegal de datos se encuentra entre la duda y la inseguridad jurídica para el ciudadano. Los ciudadanos podrán exigir la rectificación de sus datos sin perjuicio de las disposiciones sobre secreto de Estado y de la Justicia.

No existe ley que regule el secreto de Estado según se ha visto en el juicio celebrado contra los «GAL» portugueses.

También la ciudadanía está desprotegida de una ley o norma referente a las escuchas telefónicas, que atañe de forma evidente al derecho a la intimidad de las personas, pues puede producir un drástico daño social, dejando claro que éstas sólo se podrán realizar bajo estricto control judicial.

JAPON

Sólo los funcionarios están sujetos a un Decreto que les prohíbe difundir datos. Las asociaciones profesionales tienen un código ético que no pueden impedir el tráfico y comercio de informaciones personales.

Desde 1988 existe un Decreto para la protección de datos personales procesados por computadoras en los órganos administrativos del Estado. Este Decreto sólo se aplica a los funcionarios, prohibiéndoles difundir cualquier tipo de información personal.

Las Compañías de Seguros también tienen códigos éticos.

AUSTRIA

La protección de datos personales en Austria se rige por la Ley de 18 de octubre de 1978.

BELGICA

Tiene el Parlamento un proyecto de Ley para obligar a los comerciantes a considerar confidencial las informaciones comerciales y a no facilitar datos sobre clientes sin permiso de los interesados. Dicho proyecto de Ley, está promovido con carácter urgente para llenar el vacío existente en torno a la protección de sus ciudadanos frente a los llamados «delitos informáticos», motivado sin duda, por la presión pública.

Propone que se obligue a los agentes comerciales a preservar el carácter confidencial de la información de sus clientes y prohíbe la tramitación de datos sin permiso a otras empresas.

La urgencia del proyecto de ley viene dada, por el «affaire Bristel». Bristel fue un joven belga que en 1990 logró entrar en el Banco de datos del primer Ministro y tuvo acceso a la información confidencial de todo el Gabinete.

CONTEXTO EUROPEO

Existe un Convenio para la protección de las personas con respecto al tratamiento automatizado de datos personales del Consejo de Europa de 28 de enero de 1981, ratificado por España el 27 de enero de 1986, así como, una serie de directrices.

BIBLIOGRAFIA

1.– Proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal. Boletín Oficial de las Cortes Generales n.º 59-1.

2.– Actas del Congreso de Informática y Derecho en Guatemala. Marzo 1982.

3.– Investigación fiscal de las cuentas bancarias. JOSÉ ANGEL ABAD. 1992.

4.– Los españoles inermes ante la venta de su intimidad. JOSÉ LUIS SEMPRÚN. 1992.

5.– La intimidad al descubierto. BALLESTEROS. 1991.

6.– La pecera informática. Editorial de ABC.

7.– El Secreto profesional médico. Revista Médico. 1991.

8.– El Delito informático. LUIS CAMACHO. 1987.

9.– Revistas informáticas. Números varios.

10.– Estudios sobre la Constitución Española. MARTÍN RETORTILLO. 1990.

Valoración española del proyecto de directiva comunitaria sobre protección de datos (Contribución al estudio de la noción de posición nacional)[1]

SANTIAGO RIPOL CARULLA

Profesor Titular de Derecho Internacional Público y Relaciones Internacionales. Universidad Pompeu Fabra de Barcelona (ESPAÑA)

INTRODUCCION

1. El 27 de julio de 1990, la Comisión Europea adoptó un «paquete» de propuestas de Directivas relacionadas con la cuestión del tratamiento automatizado de los datos de carácter personal.

La primera propuesta, preparada por la Dirección General III (Mercado Interior), se refiere a los principios generales en materia de protección de datos personales [2]; la segunda, en cambio, cubre tan sólo la protección de los datos personales y la intimidad en el contexto de las redes públicas digitales de telecomunicación y fue preparada por la DG XIII (Telecomunicaciones, Industrias de la Información e Innovación) [3]. Una y otra con

[1] Este trabajo se inscribe en el conjunto de una investigación más amplia sobre «El derecho de la protección de datos», que se desarrolla gracias a la ayuda del Centre d'Estudis Jurídics i Formació Especialiltzada, de la Generalitat de Catalunya. Resolución de septiembre de 1991.

[2] Propuesta de Directiva del Consejo relativa a la Protección de las personas en lo referente al tratamiento de datos personales. COM (90) 314 final – SYN 288. En «DOCE», n.º C 277, de 5 de noviembre de 1990, pp. 3-12.

[3] Propuesta de Directiva del Consejo relativa a la protección de los datos personales y

base jurídica en el artículo 110 A del Tratado constitutivo de la CEE, el cual hace referencia a las «medidas relativas a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior».

De esta forma la Comisión ejercía su capacidad para iniciar el proceso de toma de decisiones comunitario en torno a un tema de importancia creciente en la vida de la Comunidad.

En opinión de la Comisión «el mercado interior implicará un espacio sin fronteras», de modo que las «administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, se ven en la creciente necesidad de colaborar e intercambiar datos personales a fin de cumplir su misión y ejecutar diferentes cometidos por cuenta de las administraciones de otros Estados miembros», y ejemplifica:

– la movilidad de las personas dentro del espacio comunitario creará nuevas necesidades para los ciudadanos europeos en lo que se refiere a la seguridad social: solicitud de reembolso o pago de subsidios por parte de los centros del país de origen y necesidad de información y consejo;

– tras la supresión de las fronteras comunitarias derivadas del establecimiento del mercado interior, el control de las mercancías en tránsito no podrá seguir efectuándose en los puestos fronterizos nacionales;

– del mismo modo, la supresión de las fronteras intracomunitarias alterará los procedimientos fiscales actuales sobre el IVA y los impuestos especiales. Se necesitará una ayuda mutua entre las administraciones fiscales nacionales para prevenir los fraudes.

A fin de hacer frente a esta nueva situación –concluye la Comisión–, es preciso impulsar el desarrollo de redes telemáticas que conecten los bancos de datos de las administraciones nacionales en los sectores de la seguridad social, las aduanas, la fiscalidad indirecta, las estadísticas y la policía de fronteras [4].

Al socaire de estas actuaciones debe situarse, en consecuencia, la aprobación del «paquete» de propuestas de Directivas al que se hace referencia.

---

de la intimidad en relación con las redes públicas digitales de telecomunicación y, en particular, la red digital de servicios integrados (RSDI) y las redes móviles digitales públicas. «Ibid.», pp. 12-17.

[4] COMISION DE LAS COMUNIDADES EUROPEAS. DIRECCION GENERAL XIII (TELECOMUNICACIONES, INDUSTRIAS DE LA INFORMACION E INNOVACION), «La Europa de las tecnologías de la información y de la comunicación», Luxemburgo: Oficina de Publicaciones Oficiales de las Comunidades Europeas, 1991, 72 pp., en particular, pp. 50-59, en las que expone los puntos relacionados con el intercambio electrónico de datos (EDI) presentes en el III Programa Marco de las Actividades Comunitarias de Investigación y Desarrollo Tecnológico (1990-1994), aprobado por el Consejo de Ministros el 23 de abril de 1990.

2. En nuestra exposición se hará referencia tan sólo a la primera «propuesta». Y ello por un doble motivo: por su contenido, más general [5], y porque su aprobación ha despertado un vivo debate en el seno de la Comunidad [6].

Ahora bien, el objetivo de la comunicación que se presenta no es analizar y valorar el contenido del texto señalado, por el contrario pretende detallar la apreciación que la propuesta de Directiva ha merecido en España y, en particular, la valoración que de la misma ha formulado el Gobierno y la postura adoptada de cara a la negociación del texto definitivo. Previamente, sin embargo, resultará conveniente formular algunas consideraciones sobre el proceso decisorio actualmente vigente en la Comunidad.

I. LA FORMACION DE LA POSICION NACIONAL ESPAÑOLA

A) Consideraciones generales: la posición nacional en el proceso decisorio de las Comunidades Europeas.

3. Las Organizaciones internacionales son creadas por los Estados para la gestión de sus intereses colectivos; en consecuencia, los órganos que las componen se ven investidos de una capacidad normativa, cuyo ejercicio revierte en la formación de la voluntad de la propia Organización internacional, distinta ya de la voluntad de los Estados miembros.

Las características del proceso de conformación de la voluntad supraestatal varía obviamente de una Organización a otra, lo que en conjunción con otros elementos, ha permitido distinguir entre Organizaciones Internacionales de coordinación y Organizaciones Internacionales de integración pues, como recuerda el Prof. DÍEZ DE VELASCO, la opción por uno u otro mecanismo de toma de decisiones «revela habitualmente cuál es la intensidad de la solidari-

---

[5] Un análisis de esta propuesta, en «Transnational Data Report (TDR)», vol. XIII, nº 9, nov. 1990, pp. 5-8. Asimismo, ESTADELLA YUSTE, O., «The Draft Directive of the European Community Regarding the Protection of Personal Data», «International and Comparative Law Quarterly (ICLO)», vol. 41, Jan. 1992, pp. 170-179, y HOLMES, B. P., «US Critizes EC Data Directive's Potencial Burdens and Barriers», «TDR» vol. XIV, n.º 6, Nov/Dec. 1991, pp. 8-9, quien ofrece una valoración norteamericana del proyecto de Directiva.

[6] En este sentido, merece la pena consultar las Actas del European Forum of IT & T Users Conference, celebrado en Bruselas los días 6 y 7 de julio de 1992 bajo el título genérico «European Networking in the 90's», y en el que pude participar en calidad de miembro español del Grupo de Trabajo sobre Protección de Datos Personales de la «Confederation of European Computer User Associations». Durante las sesiones de trabajo, fue presentado el Informe elaborado por los miembros del citado Grupo de Trabajo («Report of the Working Group of Confederation of European Computer Users Associations (CECUA) on the Proposed Directive on the Protection of Privacy of Individuals in Regards to the Processing of Personal Data»), donde se analiza el articulado de la propuesta de Directiva y se recomiendan cambios ahí donde se estima necesario. Ver, FITZGERALD, M., «Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data. An Industry View», en EUROPEAN FORUM OF IT&T USERS CONFERENCE, «European Networking in the 90's, 6/7 July 1992, Speakers Papers», pp. 97-108.

dad colectiva y en qué grado la Organización se muestra respetuosa con la libertad de los Estados miembros» [7].

4. En general, las Organizaciones Internacionales de integración, también llamadas supranacionales y de las que la Comunidad Europea es el máximo exponente [8], presentan un procedimiento especialmente atento a los intereses y a la voluntad de los Estados miembros, así como a los puntos de vista de los agentes socioeconómicos que se verán afectados directamente por sus decisiones [9].

En el caso la Comunidad Europea esta circunstancia se concreta en la nota de permeabilidad que, según se indica, caracteriza su proceso decisorio; permeabilidad a las presiones e influencias que puedan ejercerse desde el interior, o desde el exterior incluso, del propio sistema institucional comunitario, y que se ha fundamentado en causas muy diversas: «su valor como fuente de información y de experiencia, como elemento de conexión con la opinión pública europea, como filtro de los diferentes sectores nacionales, o como elemento de ordenación y coordinación de las reinvidicaciones de éstos» [10].

El resultado deberá ser un texto consensuado en sus grandes líneas y que, por lo tanto, no encontrará obstáculos en su cumplimiento. En otro orden de ideas, esta sintonía entre la voluntad de la organización y las voluntades autónomas de sus Estados miembros hará posible preservar el nivel de independencia respecto a los Gobiernos nacionales que precisa para el correcto ejercicio de su labor una institución a la que le han sido conferidas competencias tradicionalmente comprendidas dentro de los poderes soberanos de los Estados.

---

[7] DIEZ DE VELASCO, M., «Instituciones de Derecho Internacional Público», Tomo II, Madrid. Ed. Tecnos, 7.ª ed., 1990, pág. 44.

[8] Sobre la distinción entre Organizaciones internacionales de integración y de coordinación, ver, a modo de ejemplo, PASTOR RIDRUEJO, J. A., «Curso de Derecho Internacional Público», Madrid. Ed. Tecnos, 4.ª Ed., 1992, pp. 696-699, quien señala que las Organizaciones Internacionales de integración se caracterizan porque sus órganos «reciben de los miembros competencias tradicionalmente comprendidas dentro de los poderes soberanos de los Estados, a cuyo ejercicio éstos renuncian. Es el caso, en parte –añade–, de la Organización de las Naciones Unidas que, previa decisión del Consejo de Seguridad, pueden ejercer medidas de fuerza armada contra el Estado que haya recurrido a la amenaza o al uso de la fuerza en contravención de los principios de la Carta (...). Pero se trata, especialmente, de las Comunidades europeas (...) que constituyen, hoy por hoy, el supuesto de cooperación internacional más intenso, interesante y adelantado» (pág. 699).

[9] En este sentido, MOLINA DEL POZO, C. F., «Supranacionalidad y ordenamiento», «Revista de Estudios e Investigación de las Comunidades Europeas», n.º 1, enero-febrero 1987, pág. 125. Citado en PAU PEDRON, A., «El proceso formativo del Derecho Comunitario derivado», Madrid: Ed. Tecnos, 1988, pág. 118.

[10] En este sentido, CIENFUEGOS, M., «La participación de los grupos de presión comunitarios en el proceso decisorio de las Comunidades Europeas», en «Comunidades Autónomas y Comunidad Europea. Relaciones jurídico-institucionales», Valladolid: Cortes de Castila y León, 1991, pp. 161-179, en particular, pp. 167-169, en las que recoge y desarrolla brevemente la nota de permeabilidad. Un examen más detallado de la misma, en AYBERK, U., «Le mécanisme de la prise des décisions communautaires en matiére de relations internationales», Bruxelles: Bruylant, 1978, pp. 48 y ss.

En consecuencia, puede decirse que el proceso de toma de decisiones vigente en la Comunidad Europea se halla repleto de mecanismos destinados a posibilitar que todos y cada uno de los Estados miembros engarcen en el texto su particular punto de vista.

Estos mecanismos se hallan en los inicios del procedimiento, pues los Estados conocen y valoran las previsiones normativas de la Comisión gracias a la publicación de informes, libros blancos y programas. Están presentes igualmente en la fase de preparación de la propuesta, ya que en el seno de la Comisión los trabajos se desarrollan por medio de Comisiones de expertos en las que figura un representante de cada Estado miembro. Pero, sin duda, la fase en que más claramente se aprecia la existencia de estos mecanismos de formación y expresión de la posición nacional de los Estados es la fase de aprobación del texto normativo, en cuyo desarrollo se ha canalizado la participación de representantes de cada país miembro a través de los Grupos de trabajo del Consejo, de las reuniones del Comité de Representantes Permanentes (COREPER) y, por fin, del Consejo de Ministros.

Esta voluntad de los Estados miembros –su posición nacional se concreta en un determinado criterio, que es mantenido, aunque con posibles modificaciones de matiz, a lo largo de todo el proceso normativo [11].

B) La formación de la posición nacional española ante la propuesta de Directiva sobre protección de datos personales (Com (90) 314).

5. La posición nacional española ante la propuesta de Directiva sobre protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal se ha concretado a raíz de diversas reuniones celebradas por altos funcionarios de los Ministerios afectados en principio por el contenido de la propuesta de directiva – Justicia, Asuntos Exteriores, Sanidad y Consumo, Relaciones con las Cortes, Administraciones Públicas y Economía y Hacienda– y por los expertos (funcionarios a su vez de tales Ministerios) que formaron parte en las reuniones de la Comisión, ordinariamente los mismos que participan en los grupos de trabajo del Consejo.

La Secretaría de Estado para las Comunidades Europeas (SECE) ha actuado como coordinadora de estas reuniones, convocándolas por lo general con el objeto de preparar la posición española ante una próxima sesión de un Grupo de trabajo del Consejo. La convocatoria, además de fijar el orden del día, suele acompañarse de los principales puntos a debatir.

Por lo general, las sesiones se han dedicado al análisis particularizado de cada artículo de la propuesta de Directiva. Al hacerlo, éstos fueron examinados a la luz del ordenamiento español. De igual modo, se tuvieron en

[11] PAU PEDRÓN, A., «El proceso... Op. cit.», pp. 119-122. Ver asimismo, GONZÁLEZ SÁNCHEZ, E., «El procedimiento decisorio comunitario. Participación de las Administraciones nacionales. Referencias al caso español», «Revista de Instituciones Europeas», vol. 14, n.º 3, 1987, pp. 687-718.

cuenta los intereses y las preocupaciones de carácter nacional de todo tipo. Con todo, las primeras reuniones partían de un estudio elaborado por la Secretaría General Técnica del Ministerio de Justicia –Puntos principales para la negociación de la Directiva Comunitaria sobre Protección de Datos Personales (SYN 288), al que se acompaña de un texto alternativo a la propuesta– que permitió identificar los principales puntos de negociación.

II. VALORACION ESPAÑOLA DE LA PROPUESTA DE DIRECTIVA COMUNITARIA SOBRE PROTECCION DE DATOS PERSONALES

A) Una valoración general de carácter positivo.

6. Como es sabido, España es uno de los cinco países comunitarios que en la actualidad carece de una ley sobre protección de las personas respecto al tratamiento automatizado de los datos de carácter personal. Esta circunstancia no supone, sin embargo, una inhibición absoluta de las autoridades españolas en relación a esta cuestión, pues, entre otras cosas, España cuenta con una legislación sectorial sobre el tema y está pronta la promulgación de una ley general sobre protección de datos. En cualquier caso, esta situación de partida marca de forma sustancial la posición española ante el Proyecto de directiva comunitaria sobre protección de datos personales [12].

Esta carencia de legislación general sobre el tema permite comprender, por ejemplo, que España valore muy favorablemente la aprobación de una Directiva que revise al alza el nivel de protección otorgado por el Convenio número 108 del Consejo de Europa, del que es parte. Las autoridades españolas son conscientes de que, con el tiempo, el Convenio ha consagrado una disparidad de niveles de protección que conviene rectificar. Asimismo, califican de forma positiva el momento de la propuesta de la Comisión, pues consideran que la aprobación de una Directiva sobre protección de datos personales es un elemento imprescindible para la construcción del mercado interior en el sector del mercado de la información.

B) Acompañada de ciertas consideraciones críticas.

7. Con todo, esta apreciación positiva de la oportunidad y de la finalidad de la propuesta de Directiva se ve acompañada de ciertas consideraciones críticas, encaminadas esencialmente a mejorar el contenido de un texto con cuyas líneas generales se está básicamente de acuerdo.

A fin de exponer de la forma más sistemática posible la postura española ante la propuesta de la Comisión que se examina, estimamos oportuno reconducir las principales matizaciones españolas a la Directiva sobre protección de datos tal y como está redactada en la actualidad a tres grupos.

---

[12] En relación a esta cuestión, ver, RIPOL CARULLA, S., «EC Data Privacy Legislation. Spanish Point of View», «Computer Fraud & Security», March, 1992, pp. 13-17.

i) En busca de un texto de mayor precisión.

8. En primer lugar, se entiende oportuno precisar el objeto de algunos pasajes del texto. A modo de ejemplo, pueden señalarse los artículos que hacen referencia a la determinación del ámbito de aplicación de la directiva, en particular, las nociones de «datos personales» y de «procesamiento».

En relación a la primera, convendría especificar si la Directiva se refiere únicamente a los datos relativos a las personas físicas, o también a las personas jurídicas, e incluso, si podría aplicarse a colectivos sin personalidad jurídica. En relación a la segunda cuestión señalada, se duda de la conveniencia de definir el término «procesamiento» mediante la enumeración de una lista cerrada de las operaciones que comporta esta actividad.

Paralelamente, España considera conveniente modificar los términos en los que ha quedado redactado el artículo 3 de la propuesta de Directiva y, en concreto, la frase final de su párrafo primero, en virtud de la cual las disposiciones de la propuesta de Directiva no serán aplicables a «los ficheros del sector público cuyas actividades no estén comprendidas en el ámbito de aplicación del Derecho comunitario».

En opinión de las autoridades españolas, esta exclusión es a todas luces insuficiente. España considera que si con ello se quieren excluir las materias de policía, seguridad interior y exterior o defensa, esta exclusión debería hacerse de forma expresa.

ii) Que regule de forma menos pormenorizada los resultados normativos a alcanzar.

9. Por otro lado, España considera que la redacción actual de la propuesta contiene elementos que podrían otorgar a las autoridades comunitarias unas prerrogativas excesivamente amplias, de ahí que algunas de sus propuestas de modificación puedan agruparse en torno al doble objetivo de limitar las competencias que se reconocen a las autoridades comunitarias y de ampliar las potestades que corresponden a los Estados.

En este sentido, cabe señalar, a modo de ejemplo, que España considera conveniente la supresión de las referencias, frecuentes en el texto de la Directiva –artículos 5 b), 9 y 17 a la noción de «ley» interna–, pues se entiende que en ningún caso es competencia del ordenamiento comunitario el precisar el rango o el alcance de las normas internas que regulan un determinado sector de actividad. Ante el riesgo de una posible interpretación de este tipo, se estima conveniente sustituir toda referencia a la noción de «ley» por un término más amplio, el de «disposición normativa», por ejemplo, que deje en manos de los Gobiernos la determinación de la norma en cuestión.

10. Mayor importancia que el aspecto señalado en el párrafo anterior presenta la actual redacción del artículo 30, respecto al cual la posición española es especialmente crítica.

España entiende que el Comité consultivo de la Comisión al que se refiere este artículo ha de poseer una naturaleza distinta, pues, de atender la Decisión del Consejo, de 13 de julio de 1987, por la que se establecen las modalidades del ejercicio de las competencias de ejecución atribuidas a la Comisión [13] , cabe deducir que, de constituirse el Comité al que se refiere el artículo 30 con las funciones que le corresponden en la actual redacción del proyecto, el peso del proceso decisorio recaería prácticamente de forma exclusiva en la Comisión.

En opinión de las autoridades españolas esta posibilidad debe evitarse, para lo cual se propone la sustitución del Comité previsto por un Comité que actúe sobre la base del procedimiento III b) de la Decisión citada. Ello permitirá un control sobre los actos de la Comisión, habida cuenta de que en el caso de que el dictamen del Comité sea contrario a la propuesta de la Comisión, o en el supuesto de que éste no llegue a emitirse, el proceso de toma de decisiones quedará paralizado momentáneamente. La propuesta deberá entonces dirigirse al Consejo, el cual deberá pronunciarse sobre ella por mayoría cualificada en un plazo de tres meses. Si transcurridos los tres meses, el Consejo no se ha pronunciado sobre las propuestas que le fueron planteadas, la Comisión estará habilitada para adoptar las medidas propuestas, excepto en el supuesto de que el Consejo haya votado en contra de sus propuestas por mayoría simple.

11. Por lo demás, España considera que esta limitación de la capacidad de actuar de las autoridades estatales no proviene exclusivamente de la amplitud de las potestades que se le reconocen a la Comisión. Lejos de ser así, se entiende que en determinadas ocasiones esta restricción de la capacidad de los Estados miembros viene determinada por el rigor con la que la propuesta de Directiva protege los intereses de los particulares, circunstancia que se aprecia en especial en la redacción de su artículo 9, que establece la obligación de informar al sujeto afectado de cualquier operación que se realice con sus datos.

En este sentido, debe indicarse que la Asociación Española de Marketing Directo considera de gran importancia proceder a una precisión del concepto

---

[13] Decisión 87/373/CEE del Consejo por la que se fijan las modalidades de ejercicio de las competencias de ejecución conferidas a la Comisión. DOCE, n.º L 197, de 18 de julio de 1987, pág. 33. Para un análisis de esta Decisión y sobre los problemas que la acompañan, ver, entre otros, ALONSO GARCÍA, E., «Los poderes de ejecución de la Comisión y la falta de legitimación activa del Parlamento para ejercitar la acción de anulación ante el Tribunal de Justicia (El nuevo artículo 145.3 del Tratado CEE, la Decisión 87/343 de 13 de julio y la Sentencia (302/87) de 27 de septiembre de 1988: A la búsqueda del nuevo equilibrio institucional entre la Comisión, el Consejo y el Parlamento tras el Acta Unica», Noticias/CEE, n.º 62, 1990, pp. 125-136, en particular, pp. 129-131; EHLERMANN, C-D., «Compétences d'exécution conférées à la Commission – La nouvelle Décision cadre du Conseil», Révue du Marché Commun, n.º 316, avril 1988, pp. 232-239; MANGAS MARTÍN, A., «El Acta Unica Europea y las modalidades de ejercicio de las competencias de ejecución atribuidas a la Comisión», Revista de Instituciones Europeas, 1988, n.º 3, pp. 789-806.

de «primera comunicación», pues si se considera que en el mismo se incluye la transferencia o el alquiler de un listado, el artículo 9 resultará de imposible cumplimiento, ya que sería costosísimo para la empresa de marketing directo remitir una información de este tipo a cada sujeto de la lista alquilada.

iii) Algunas propuestas de modificación motivadas por intereses específicos del Gobierno español.

12. El tercer núcleo de apreciaciones críticas responde a intereses específicos del Gobierno español.

Así, se propone la modificación de la actual redacción del artículo 15.3, por el cual se contempla la posibilidad de excepcionar mediante ley los derechos del afectado recogidos en los epígrafes 3 y 4 del artículo 14: derecho a obtener periódicamente comunicación de los datos obtenidos en ficheros automáticos que afecten a su persona.

La administración española considera imprescindible limitar el derecho citado en el ámbito de los ficheros tributarios, por cuanto se considera que un acceso ilimitado del contribuyente a los datos que sobre su persona obran en poder de la Administración tributaria (particularmente de los suministrados por terceras personas) ofrecería la posibilidad de efectuar sus declaraciones con ocultación total o parcial de aquellos hechos imponibles, datos o circunstancias respecto de los cuales se tiene constancia que no son conocidos por la Administración.

13. Paralelamente, se postula la modificación de los artículos 27 y 30 de la propuesta, referentes a la creación de un Grupo de protección de datos personales y de un Comité consultivo, respectivamente.

El interés por su modificación se justifica básicamente en la organización territorial de la administración española en 17 Comunidades Autónomas y responde al interés de las autoridades españolas de evitar posibles controversias futuras entre sus administraciones central y periféricas. A estos efectos, se cree conveniente especificar que el Grupo de trabajo y el Comité consultivo a los que hacen referencia los artículos citados están compuestos por un único representante de las autoridades de supervisión de cada Estado miembro.

CONSIDERACIONES FINALES

14. A modo de conclusión, pues, podría señalarse que la posición española ante el proyecto de directiva que regula la protección de los individuos en relación con el proceso de datos personales aunque es básicamente positiva posee puntos de crítica nada despreciables.

Como ha podido apreciarse quizás la objeción más importante de las señaladas es la que considera que el texto tal y como está redactado actualmente es excesivamente pormenorizado. Las autoridades y los diferentes

agentes de los sectores de producción españoles relacionados con el tema consideran que un texto armonizador, como pretende ser la Directiva, no debería especificar con tanto detalle el resultado normativo que se quiere alcanzar. Por el contrario debería dejar mayor capacidad de decisión a las autoridades de los Estados miembros.

Por esta razón, se valora positivamente que en el proyecto se haya incluido un artículo, el 20, mediante el cual se fomenta la elaboración de códigos de conducta, con los que atender mejor las especifidades de cada sector profesional. En cualquier caso, se considera que para permitir un desarrollo positivo y profundo de esta técnica normativa la legislación general, esto es, la Directiva debería ser más abierta y general.

15. En definitiva, cabe señalar que las apreciaciones críticas que desde España se formulan a la propuesta de Directiva obedecen en buena medida a la escasa tradición de ordenación de esta materia.

Efectivamente, únicamente de atender esta circunstancia es posible comprender que la postura española alterne críticas que postulan una mayor concreción del articulado del proyecto con propuestas de modificación del texto encaminadas a rebajar el nivel de pormenorización de algunos de sus artículos.

La posición española en relación con la propuesta de Directiva sobre protección de datos personales se mueve, así, en un doble interés: buscando que la normativa comunitaria garantice el nivel de protección suficiente al ciudadano español y el intercambio fluido de datos informatizados entre los países comunitarios, y que sea, a la vez, más respetuosa con la capacidad legislativa de los Estados miembros.

Protección de las personas respecto al tratamiento automatizado de datos personales. Normativa Europea. Proyecto de Ley Española

RUBÉN SÁENZ GIL
Licenciado en Derecho
(ESPAÑA)

SUMARIO

1. INTRODUCCION
2. CONVENIO DEL CONSEJO DE EUROPA
3. PROTECCION DE DATOS PERSONALES Y COMUNIDAD EUROPEA
4. PROYECTO DE LEY ESPAÑOLA DE PROTECCION DE DATOS
5. CONCLUSIONES
6. BIBLIOGRAFIA

1. INTRODUCCION

La dignidad humana supone el principio que fundamenta los derechos a la intimidad, al honor y a la propia imagen.

Actualmente, no basta con pensar en el derecho a la intimidad como un derecho de defensa frente a todo tipo de invasión indebida en la esfera pri-

vada, sino que también, debe comprenderse como un derecho activo de control sobre el conjunto de datos que atañen a una persona [1].

Esta ampliación del concepto de derecho a la intimidad, ha permitido que en nuestros días se recurra a este derecho para tratar de solventar jurídicamente algunos de los problemas de nuestra sociedad, como el de las repercusiones sociales de las que se han venido a llamar nuevas tecnologías de la información.

El derecho a la intimidad se halla recogido como derecho fundamental en el artículo 12 de la Declaración Universal de los Derechos Humanos y en el artículo 8 del Convenio Europeo de 1950.

También la Constitución Española de 1978, en su artículo 18.1 reconoce «el derecho al honor, la intimidad personal y familiar y a la propia imagen.»

Y en el apartado 4 del citado artículo se dice que: «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

En efecto, el avance y la generalización de las nuevas tecnologías de la información puede suponer una amenaza para el derecho a la intimidad. Y esto debido a la capacidad casi ilimitada de la tecnología informática para almacenar información, relacionarla y sistematizarla. De este modo la información sobre la identidad o las circunstancias de las personas puede ser registrada en soportes informáticos, combinarse y convertirse en nuevas informaciones. Además estos datos pueden transmitirse sin que las personas a que se refieren sean conscientes de ello.

Según M. HEREDERO HIGUERAS [2], con la generalización de las tecnologías de la información aparecen dos claros riesgos para la persona:

– La obtención de información sobre sus circunstancias sin su conocimiento.

– El uso indebido de esa información, o el uso de la obtenida lícitamente, para otros usos de los que justificarían su obtención. Los datos personales almacenados en ficheros informáticos pueden transferirse con gran facilidad. Esa transmisión puede darse de unos países a otros, dando lugar a flujos internacionales de datos.

A toda esta problemática se le han intentado buscar respuestas jurídicas. A esto se debe el desarrollo en las legislaciones más actuales de las «leyes de protección de datos». La primera ley de protección de datos fue la Ley de Hesse de 1970. Durante los años setenta se suceden numerosas leyes de protección de datos en países como Suecia, U.S.A., Francia, Reino Unido,

[1] PÉREZ LUÑO, A. E., «Derechos Humanos, Estado de Derecho y Constitución», Madrid, 1991.

[2] HEREDERO HIGUERAS, M., «La protección de datos personales registrados en soportes informáticos», en Revista de Informática para Juristas, n.º 2, enero de 1992, p. 2.

etc. Incluso algunos países incluyen en sus Constituciones normas relativas a la utilización de la informática en casos de datos personales. Este es el caso de la Constitución de la República Portuguesa en su artículo 35 y el de la Constitución Española en su artículo 18.4, el cual antes hemos reproducido.

2. CONVENIO DEL CONSEJO DE EUROPA

Tras dos resoluciones del Comité de Ministros del Consejo de Europa sobre protección de datos en los años 1973 y 1974 que ya tratan de orientar tímidamente el camino a seguir en esta materia [3]. El 28 de enero de 1981 es aprobado por el Consejo de Europa el «Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, Convenio publicado en 1985 en el BOE [4].

Como podemos observar en la denominación de este Convenio se opta por hablar de «protección de las personas» en vez de «protección de datos». Pues este último término ha sido frecuentemente criticado en el sentido de que lo que realmente se trata de proteger son las personas y no los datos referentes a ellas.

Según el artículo 1 del Convenio su fin es garantizar a las personas físicas en el territorio de cada Estado Parte, el respeto de sus derechos y libertades fundamentales, y en especial su derecho a la vida privada respecto al tratamiento automatizado de sus datos personales.

Su artículo 2 define datos personales como «cualquier información relativa a una persona física identificada o identificable».

El artículo 3 establece que se aplicará a ficheros informatizados en los sectores público y privado.

El Convenio es una norma mínima, pueden existir normas internas más favorables, como puede desprenderse de su artículo 11.

Para este Convenio los datos personales sometidos a tratamiento automatizado deben:

– Registrarse para finalidades legítimas.

– Ser puestos al día y exactos.

– Y recogerse con garantías si revelan el origen racial, religión, ideología o se refieran a la salud o vida sexual de los afectados.

---

[3] Respecto a estas resoluciones ver: HONDIUS, F., «La protección des données en Europe. Un example de coopération legislative», Ici l'Europe, supplement juridíque núm. 12, avril 1975, p. 20.

[4] Boletín Oficial del Estado de 15 de Noviembre de 1985, p. 36000.

En el artículo 9 se prevén excepciones y restricciones.

Estas caben cuando:

– Estén previstas en la legislación del Estado en cuestión.

– Sean necesarias en un marco democrático.

– Se protejan intereses públicos.

– O se favorezca la represión de infracciones penales.

El capítulo III se refiere a «flujos transfronterizos de datos», estableciendo el principio de libre circulación de informaciones entre los Estados parte del Convenio, aunque en el artículo 12 se establecen dos excepciones:

– Que una parte prevea una reglamentación específica para determinados tipos de datos personales y la otra parte no la prevea.

– Que la transmisión de información se dirija a un Estado no contratante.

También podemos encontrar en los artículos 13 y 14 unos mecanismos de protección del Convenio:

– La cooperación entre los Estados que se concreta en personas de cada Estado contratante.

– El Comité Consultivo, el cual tiene potestad para presentar propuestas de modificación del Convenio y para opinar sobre él.

El profesor RIPOLL CARULLA pone de relieve el carácter armonizador del Convenio del Consejo de Europa, «pues su artículo 11 al posibilitar que los Estados parte ofrezcan una protección más amplia a la recogida en el texto del Tratado, reconoce implícitamente su voluntad armonizadora» [5].

Respecto al ámbito de aplicación del Convenio, el profesor GARZÓN CLARIANA critica la facultad concedida a los Estados miembros de sustraer de la aplicación del Convenio a categorías de archivos automatizados. Y además señala GARCÓN, «esta vía puede llevar en la práctica, a la reducción de las categorías de archivos del sector público afectadas por el Convenio» [6].

Otras autorizadas críticas son las realizadas por el profesor PÉREZ LUÑO, así destaca las débiles competencias del Comité Consultivo. También este

[5] RIPOLL CARULLA, S., «El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: balance a los siete años de su apertura a la firma», Congreso sobre Derecho informático, Zaragoza, Facultad de Derecho, 1989, p. 398.

[6] GARZÓN CLARIANA, G., «La protección de los datos personales y la función normativa del Consejo de Europa, Revista de Instituciones Europeas, 181, n.º 1, p. 17.

autor señala la inconveniencia de la remisión a los Estados parte el procedimiento de recursos y el aparato sancionador [7].

Pese a todas estas críticas, conviene resaltar que la aprobación del Convenio al que nos estamos refiriendo supuso un avance en la unificación de criterios en esta materia.

Además el Comité Consultivo a través de reuniones de expertos en esta materia ha trabajado en la línea de perfeccionar el Convenio [8].

El Convenio del Consejo de Europa ha sido ratificado por Francia, Reino Unido, Irlanda, Suecia, Noruega, Austria, R. F. Alemana, Dinamarca, Luxemburgo y España. España es parte del Convenio desde 1985, aunque todavía no existe ley interna sobre protección de datos.

3. PROTECCION DE DATOS PERSONALES Y COMUNIDAD EUROPEA

Mientras la transmisión internacional de datos va en aumento, en los países de la Comunidad Europea se hace necesaria una armonización en materia de protección de datos que todavía no se ha conseguido. Según la C.N.I.L. francesa:

«Viendo las disparidades de las soluciones nacionales, sería de temer que el denominador común de protección en el espacio europeo, donde ya se multiplican los intercambios de información, se establezca en el nivel más bajo de protección» [9]. El 18 de julio 1990, la Comisión de la Comunidad Europea adopta una comunicación sobre protección de las personas en lo referente al tratamiento de datos personales y a la seguridad de los sistemas de información, [10] la cual contiene las siguientes propuestas de:

– Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales.

– Resolución de los representantes de los Gobiernos de los Estados miembros para ampliar la aplicación de estos principios a los ficheros de las administraciones cuyas actividades no entran en el campo del Derecho comunitario.

– Resolución para la negociación de la adhesión de las Comunidades Europeas al Convenio del Consejo de Europa de 1981.

---

[7] PÉREZ LUÑO, E., «La Incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español», en el vol. de M. LOSANO, A. E. PÉREZ LUÑO, M.F. GUERRERO MATEUS, Libertad informática y Leyes de protección de datos pesonales, Centro de Estudios Constitucionales, Madrid, 1989, p. 174.

[8] Consejo de Europa. «Legislation and data protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation», Rome, 1983.

[9] C.N.I.L., Commision Nationale de l'Informatique et Libertés, 11.º rapport d'activite (1990). Ed. Documentation Française, París 1991.

[10] DOC 277 de 5-11-1990 y Bol. CE 11-1990 , punto 1.3.194.

– Directiva del Consejo relativa a la protección de los datos personales y de la intimidad en lo referente a las redes públicas digitales de comunicación, y especialmente a la red digital de servicios integrados (R.D.S.I.) y las redes móviles digitales públicas.

– Decisión del Consejo relativa a la seguridad de la información. En esta comunicación la Comisión considera necesaria la protección de las personas frente al tratamiento automatizado de datos personales en el ámbito de la Comunidad Europea. La Comisión propone un planteamiento conjunto, frente a los diferentes planteamientos nacionales, dirigido a promover una política activa en el campo de la seguridad de los sistemas de información y a garantizar un alto nivel de protección en todos los Estados miembros.

El dictamen del Comité Económico y Social se ha mostrado favorable respecto a la comunicación. Este destaca la gran importancia del alto nivel de protección de datos defendido en la comunicación. Respecto a la primera propuesta de directiva, la principal de todas ellas, este dictamen remarca que el tratamiento de los datos personales del sector público debe someterse antes a un examen llevado a cabo por autoridades públicas independientes designadas para controlar la protección de datos.

La propuesta de la Comunidad Europea ha sido objeto de múltiples comentarios tanto favorables como desfavorables. Por ejemplo Estados Unidos y otros Estados no comunitarios, dadas las diferencias de las leyes de protección de datos americanas, de tipo sectorial, respecto a las europeas, de tipo generalista, han criticado las restricciones a la transmisión de datos a Estados no miembros de la Comunidad en caso de distintos niveles de protección.

Esta propuesta debido a las dificultades que puede presentar su definitiva aprobación con un contenido como el actual, seguramente sufrirá algunas modificaciones antes del acuerdo del Consejo europeo.

4. PROYECTO DE LEY ESPAÑOLA SOBRE PROTECCION DE DATOS

En nuestro país existen normas sectoriales referentes a la informática y libertades [11], aunque todavía no se ha promulgado una ley general interna sobre protección de datos. Sí que existe un «Proyecto de Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal», LORTAD [12].

Esta Ley Orgánica es un desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, según se señala en su artículo 1.

---

[11] PÉREZ LUÑO, E., «La Incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español», en el vol. de M. LOSANO, A. E. PÉREZ LUÑO, M. F. GUERRERO MATEUS, Libertad informática y leyes de protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1989, p. 187.

[12] Boletín Oficial de las Cortes Generales, n.º 59-1, de 24 de julio de 1991.

Según su artículo 2, la Ley se aplica a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado. Y a continuación este artículo establece unas excepciones. El Título Segundo se dedica a los «principios de la protección de datos». En el artículo 4, se exige que los datos sean adecuados a las finalidades para las que se hayan obtenido, se utilicen sólo para estas finalidades y sean exactos. También se ofrecen garantías para los datos relacionados con la ideología, religión, creencias, origen racial o vida sexual del afectado.

En el Título Tercero se recogen entre otros el derecho de información del afectado respecto a sus datos personales contenidos en ficheros automatizados, el derecho a rectificar datos inexactos, el derecho a conocer la existencia de ficheros automatizados, etc.

El Título Cuarto se refiere a características de los ficheros públicos y privados. Mientras el Título Quinto exige para la transferencia internacional de datos que exista en el país destinatario una protección equiparable a la «presente ley».

En el Título Sexto, se crea la agencia de Protección de Datos, «será un ente de Derecho Público, con personalidad propia y plena capacidad pública y privada», que actuará con plena independencia de las Administraciones Públicas.

Entre sus funciones podemos citar: el velar por el cumplimiento de la legislación sobre protección de datos, el atender peticiones de afectados, el ejercer la potestad sancionadora, etc.

El Título Séptimo establece las infracciones y sanciones, estas últimas podrán oscilar entre 100.000 y 100 millones de pesetas y en caso de funcionarios también se aplicará el régimen disciplinario de las Administraciones públicas. Se sancionarán, por ejemplo, las filtraciones de datos contenidos en los ficheros públicos a las empresas privadas.

La LORTAD ha recibido numerosas enmiendas, entre las que destacan además de las de los grupos parlamentarios, las de la Comisión de Libertades e Informática (CLI).

Algunas de éstas tratan de adaptar el Proyecto a la normativa europea.

Para evitar el acceso a los ficheros informáticos públicos o privados por parte de personas no autorizadas, será conveniente que sus responsables sepan protegerlos.

La mejor forma de proteger un fichero informático es mediante la criptología.

Protegido el fichero con un programa encriptador, se tiene la certeza de que sólo tendrán acceso al fichero quienes conozcan la clave.

Del texto del Proyecto de Ley puede inferirse que será imprescindible el registro de cualquier fichero de datos personales público o privado. Se creará un Registro General de Protección de Datos, que estará facultado para inspeccionar los ficheros.

Según el artículo 38 del Proyecto de Ley este Registro General estará integrado en la Agencia de Protección de Datos. Por tanto parece que ésta tendrá un gran poder. Y será su labor la que principalmente va determinar las consecuencias de la futura ley.

5. CONCLUSIONES

El desarrollo de las tecnologías de la información conlleva una amenaza para el derecho a la intimidad, derecho sustentado por la propia dignidad humana.

En la búsqueda de una solución el Consejo de Europa adopta en 1981 un «Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal». Este Convenio trata de compatibilizar el principio de libre circulación de la información entre los Estados parte y el derecho a la intimidad.

Y ha supuesto un avance significativo en la unificación de criterios en la materia.

Respecto a la propuesta de Directivas de la Comunidad Europea sobre este tema, se propone un planteamiento conjunto frente a los distintos planteamientos nacionales, para conseguir un alto nivel de protección.

En el ámbito español, la futura «Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal» habrá de ser aprobada en esta legislatura y aunque seguirá en líneas generales el texto del Proyecto al que nos hemos referido, habrá de sufrir alguna modificación para adaptarse a la normativa europea.

6. BIBLIOGRAFIA

– «Convenio para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal», Boletín Oficial del Estado de 15 de Noviembre de 1985, p. 36000.

– «Comunicación de la Comisión sobre protección de las personas en lo referente al tratamiento de datos personales y a la seguridad de los sistemas de información», DOC 277 de 5-11-1990 y Bol. CE 11-1990, punto 1.3.194.

– «Proyecto de Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal», Boletín oficial de las Cortes Generales, n.º 59-1, de 24 de julio de 1991.

– PÉREZ LUÑO, A. E., «Derechos Humanos, Estado de Derecho y Constitución», Madrid,1991.

– M. LOSANO; A. E. PÉREZ LUÑO y M. F. GUERRERO MATEUS, «Libertad Informática y leyes de protección de datos personales», Centro de Estudios Constitucionales, Madrid, 1989.

– GARZÓN CLARIANA, G., «La protección de los datos personales y la función normativa del Consejo de Europa», Revista de Instituciones Europeas, 1 81, n.º 1.

– RIPOLL CARULLA, S., «El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal: balance a los siete años de su apertura a la firma», Congreso sobre Derecho informático, Zaragoza, Facultad de Derecho, 1989.

– HEREDERO HIGUERAS, M., «La protección de los datos personales registrados en soportes informáticos», en Revista de Informática para Juristas, n.º 2, enero de 1992.

– C.N.I.L., Commision Nationale de l'Informatique et Libertés, 11.º rapport d'activite (1990). Ed. Documentation Française, París 1991.

– Consejo de Europa. Legislation and data protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation, Rome, 1983.

El tratamiento automatizado de las Bases de Datos en el marco de la Comunidad Económica Europea: Su protección

ALVARO SÁNCHEZ BRAVO

Abogado. Asesor Jurídico en materia Civil, Laboral y Comercial (ESPAÑA)

NOTA PRELIMINAR

Agradecemos a Doña Antonia Marcos Gadeo, de la Eurobiblioteca de Cádiz la colaboración y atención prestada para la elaboración de esta comunicación.

Extremadura, Verano de 1992.

1. INTRODUCCION

El uso más frecuente e intensivo del tratamiento de datos personales, unido a la necesidad de intercambio de datos hacen indispensable la aplicación en la Comunidad Europea de medidas tendentes a garantizar la protección de la intimidad de las personas en lo referente al tratamiento de sus datos personales.

Paralelamente a una imparable evolución técnica de las tecnologías de la información, la Comunidad se caracteriza por la diversidad de enfoques nacionales en el tratamiento de esta cuestión. Actualmente sólo siete Estados Miembros poseen legislación específica sobre la materia. Por añadidura, aunque con los mismos objetivos, sus legislaciones adoptan a veces soluciones divergentes.

A nivel supranacional, conviene destacar la Recomendación del Consejo de la OCDE, de 23 de Septiembre de 1980, sobre las directrices que rigen la protección de la intimidad y las transferencias transfronterizas de datos.

Por otra parte, el único instrumento de Derecho Internacional existente en este ámbito es el Convenio del Consejo de Europa, de 28 de Enero de 1981, sobre la protección de las personas en lo referente al tratamiento automatizado de datos personales, que no obstante no ha limitado esta disparidad, ya que por una parte, permite elegir entre un gran número de opciones para la aplicación de los principios básicos que define y, por otra, sólo ha sido ratificada por siete Estados miembros (Alemania, Dinamarca, España, Francia, Irlanda, Luxemburgo y Reino Unido), de los cuales España, todavía no se ha dotado de legislación interna. No obstante el propio Consejo de Europa de Estrasburgo, de los días 8 y 9 de Diciembre de 1989 destacó, al discutir ciertas medidas en favor de la libre circulación de las personas y de la Europa de los ciudadanos, la necesidad de velar porque la colaboración entre las Administraciones garantice previamente la protección de los ciudadanos por lo que se refiere a la utilización de las Bases de datos personales.

Las inquietudes ante esta situación llegaron también ante las Naciones Unidas, que están preparando actualmente sus directrices sobre la materia.

Ciñéndonos al contexto comunitario, el Parlamento Europeo ha adoptado desde el año 1977 varias soluciones en las que expresa su inquietud por el tema e invita a la Comisión a preparar una propuesta de Directiva armonizadora de las legislaciones nacionales en materia de protección de datos personales.

Por su parte la Comisión Europea, en Recomendación de 29 de Julio de 1981, subrayaba el carácter de derecho fundamental de dicha protección y recomendaba a todos los Estados miembros que ratificasen el Convenio del Consejo de Europa de 1981, antes citado. No obstante, escasa fue la repercusión de esta recomendación, que se ha visto reforzada por la Recomendación de Decisión del Consejo relativa a la apertura de negociaciones con vistas a la adhesión de las Comunidades Europeas al convenio del Consejo de Europa, adoptada el 24 de Septiembre de 1990. Este texto establece las directrices básicas para llevar a cabo tales negociaciones, que permita la conclusión de un protocolo adicional por el que se permita a la Comunidad ser parte en dicho Convenio, y garantizar así la protección y el tráfico transfronterizo de datos de carácter personal con terceros países, asegurando a las personas un nivel de protección equivalente, en los supuestos de intercambios de datos personales con los referidos países.

2. SITUACION COMUNITARIA

Dos son los grandes ámbitos que pueden definir la situación en el marco comunitario, y a las que intentan poner freno y solución las medidas comuni-

tarias adoptadas, a las que luego nos referiremos más detenidamente. Abordemos ahora esta problemática:

A. Disparidad de las legislaciones nacionales: Problemática.

La protección de las personas en lo referente a los datos personales es objeto de diversos enfoques en los Estados miembros; diversidad resultante, por un lado, de la carencia de legislación específica en algunos Estados miembros, y por otro, del diferente contenido de la legislación existente, en aquellos que la poseen.

Aunque el objeto de estas normas internas es el mismo, la protección de las personas afectadas adopta diferentes soluciones por la gran variedad de opciones posibles para asegurar tal protección. Además, los progresos técnicos pueden llevar a los socios comunitarios a adoptar diferentes pautas de actuación, y acentuar si cabe aún más, las diferencias existentes.

Esta situación genera para la Comunidad una triple problemática:

1) La ausencia de una regulación protectora por parte de los Estados miembros acerca de los datos personales contrasta con la firme y decidida importancia que la Comunidad concede al respeto de los derechos fundamentales, manifestada en la Declaración conjunta del Parlamento, Consejo y Comisión europeos de 1977, Recomendación de 29 de Julio de 1981 que subrayaba el carácter de derecho fundamental de dicha protección, y en el párrafo tercero del Preámbulo del Acta Unica Europea.

2) Los progresos técnicos registrados en el ámbito del tratamiento de la información, justifican que la circulación de datos personales sea necesaria para la efectiva creación y funcionamiento del mercado interior. Dicha circulación puede manifestarse a través de tres niveles:

a) Nivel económico. La transferencia de datos personales se manifiesta como necesaria entre los agentes económicos que mantengan actividades fronterizas, para la consecución de los objetivos que les son propios.

b) Nivel administrativo. El proceso de integración europea tiene que ir acompañado de una cooperación y colaboración entre las administraciones nacionales, para lo cual la circulación de datos se erige en condición indispensable de tal proceso.

c) Nivel científico. La cooperación científica y técnica entre los Estados nacionales constituye uno de los objetivos a desarrollar por la Comunidad. El intercambio de datos deviene así condición indispensable para la consecución de tal objetivo y lograr así un desarrollo tecnológico equivalente en los Estados miembros que elimine los desequilibrios actualmente existentes en este campo.

3) Estas diferencias pueden generar un proceso de evidente peligrosidad, el falseamiento de la competencia entre los agentes económicos privados según las restricciones a las que estén sometidos en su país. Esta cuestión

debe atajarse desde su raíz, pues constituye uno de los obstáculos fundamentales para la consecución de los objetivos comunitarios, máxime en una Comunidad de cooperación fundamentalmente económica como es ésta.

B. Necesidad de un enfoque comunitario.

Vista la problemática anterior, la ausencia de un mecanismo protector comunitario constituye una grave traba para la protección de los ciudadanos comunitarios y el desarrollo y consolidación del mercado interior.

El establecimiento de un marco común de actuación se erige así en requisito imprescindible para el desarrollo de la industria de la informática y de los servicios telemáticos.

Debe tenerse en cuenta también, que la penetración de la informática en todas las actividades económicas y la aparición de sistemas globales de comunicación, que posibilitan la interrelación de varias actividades exige por otro lado el establecimiento de un sistema de seguridad de la información adaptado a los riesgos derivados de posibles fallos, y que garantice una protección efectiva de la intimidad y preserve la integridad de las Bases de datos. No obstante, dado que los modernos sistemas de telecomunicaciones permiten intercambios de datos a nivel planetario, debe tenerse en cuenta esta posibilidad para que tal protección resulte adecuada y eficaz.

Las diferentes formas en que los Estados miembros abordan la regulación de la propiedad intelectual informática, por tener un ámbito territorial, –pueden tener por efecto impedir– si subsisten las diferencias con respecto al ámbito de aplicación, las condiciones, las excepciones y la duración de la protección la libre circulación de mercancías y servicios en la Comunidad. Debe tenerse en cuenta, que en la actualidad existe un gran desequilibrio en el nivel de inversión en el sector de las Bases de datos, tanto entre los Estados Miembros, como entre la Comunidad y los principales países productores de bases de datos del mundo.

Pero es quizás, a nivel ciudadano donde esta necesidad de regulación uniforme se muestra más imperiosa, por cuanto tal disparidad contribuye a crear evidentes desequilibrios, tanto en lo referente a la protección del derecho a la intimidad, como al ejercicio de las garantías que les son anejas.

Observamos cómo conductas perseguidas y castigadas severamente en unos países, carecen en otros de toda actividad sancionadora. Esto contribuye a que tales bases de datos sean utilizadas como a cada cual convenga a sus intereses, y posibilita que la intimidad de los ciudadanos se vea constantemente perturbada por hechos atentatorios contra su vida privada, no dotándosele, como sería su justa contrapartida, de mecanismos de defensa que le permitan ejercitar contra tal intromisión.

El derecho a la intimidad, del que el ciudadano es titular, aunque sólo en una concepción teórica, se ve despojado de las garantías que le son propias, vaciándolo de contenido y quedándolo relegado a una mera declaración rim-

bombante sin ninguna eficacia práctica. El derecho debe ser tal, no sólo por que se tenga como titular, si no porque, llegado el caso, pueda ejercitarse.

3. MARCO GLOBAL DE ACTUACION COMUNITARIA

A. Extenso ámbito de protección.

Considerando que las legislaciones internas tienen por objeto garantizar los derechos fundamentales de la persona, en particular el derecho a la intimidad y que la Comunidad ha manifestado su vinculación con los derechos fundamentales, las medidas que se adopten no deben implicar la disminución del nivel de protección, sino, al contrario, garantizar un alto nivel de protección en toda la Comunidad.

El acercamiento a un amplio y común nivel que garantice los derechos de la persona, exige por su propia naturaleza el establecimiento de un sistema eficaz de seguridad de la información. Resulta sumamente importante garantizar una efectiva y práctica seguridad de la información almacenada informáticamente, sin que ello implique diferencias entre los Estados miembros en lo referente a la investigación científica y técnica o en sus relaciones con terceros países.

Para ello se exige no sólo una actuación de carácter legislativo, sino previa y fundamentalmente un estudio pormenorizado de las necesidades y opciones que ante este proceso se presentan en la Comunidad, mediante una cooperación estrecha entre los Estados nacionales y los agentes económicos responsables del sector.

Esta vocación global de la Comunidad se ha visto en la realidad avalada por la adopción de diversas y variadas disposiciones, que vienen a regular no sólo las bases de datos, sino otros aspectos del llamado Derecho Informático, pero que guardan en sí una unidad de criterio y tratan de resolver, en lo posible, la complejidad de este fenómeno plural.

Tres grandes grupos pueden establecerse en la regulación de este fenómeno:

a) Propiedad Intelectual informática:

1. Directiva del Consejo, de 14 de Mayo de 1991, sobre la protección jurídica de los programas de ordenador.

Este texto, después de considerar a los programas de ordenador como un sector importante para el desarrollo de la tecnología informática comunitaria, establece la necesidad de eliminar las barreras nacionales que producen efectos negativos y directos sobre el funcionamiento del Mercado Común, en lo relativo a los programas informáticos; barreras que pueden acentuarse a medida que los Estados miembros legislen sobre la materia.

El marco de actuación debe limitarse por una parte, a garantizar que los países comunitarios concedan a dichos programas una protección con arreglo

a la legislación sobre derechos de autor, y por otro, establecer las pautas esenciales de su regulación; a saber: sujeto y objeto de protección, derechos exclusivos a los que pueden acogerse los sujetos de la protección para autorizar o prohibir determinados actos y la duración de dicha protección.

2. Directiva del Consejo, de 23 de Junio de 1992, relativa a la protección jurídica de las bases de datos.

El objetivo de la Directiva es establecer un regimen jurídico armonizado y estable que proteja las bases de datos creadas en la Comunidad.

Pretende solucionar los problemas específicos que se plantean como resultado de la utilización de equipos electrónicos de procesos de datos, en la recopilación, tratamiento y recuperación de la «información».

La presente Directiva sigue el principio de garantizar una protección mediante el derecho de autor, basada en cómo se ha elaborado la colección; es decir, la creación personal de autor al seleccionar y disponer el material y hacerlo accesible al usuario. Las manipulaciones no autorizadas de las bases de datos, protegidas por el derecho de autor, supone una infracción de los derechos sobre la selección y disposición de dichas bases, pero no de los derechos correspondientes a su contenido que estarán protegidos por la legislación de los Estados miembros.

Como excepción, además de proteger las bases de datos como colecciones, la Directiva protege también de forma limitada el contenido de la base de datos, cuando el mismo no está protegido por el derecho de autor.

El objetivo es fomentar la inversión en el sector de tratamiento de datos, protegiéndolo además contra la apropiación indebida y la competencia desleal. La protección mediante el derecho de autor de las bases de datos no impide la adquisición de derechos de publicación de obras o materiales, ni la creación de forma independiente de los mismos por terceros.

En conclusión, la Directiva pretende abarcar tanto el aspecto creativo como el económico de las bases de datos: la creación intelectual del autor mediante el derecho de autor, aplicable a gran número de bases de datos producidas hoy día en la Comunidad; y la inversión del creador, contra la actividad de los piratas competidores que ilícitamente pretendan apropiarse del resultado del trabajo recopilatorio efectuado por el propietario de la base de datos.

b) Bases de datos personales:

1. Directiva del Consejo, de 24 de Septiembre de 1990, relativa a la protección de las personas en lo referente al tratamiento de datos personales.

Esta Directiva «general» tiene por objeto establecer una protección equivalente de alto nivel en los Estados miembros de la Comunidad, para eliminar los obstáculos a los intercambios de datos, necesarios para la consecución

del mercado interior. Esta labor necesita que los Estados nacionales garanticen los principios enunciados en la misma.

Tales principios se refieren a las condiciones que determinan la legitimidad del tratamiento de datos personales, derechos del interesado (derecho de información, acceso, oposición, rectificación), calidad de los datos (exactitud, recogida lícita, registro con fines determinados y legítimos) y creación de un Grupo de Protección de Datos Personales que garantice el respeto de tales principios.

La Directiva incluye los ficheros del sector privado y público cuyas actividades esten sujetas al Derecho Comunitario.

Los Estados miembros no podrán imponer restricciones a la circulación de dichos datos dentro de la Comunidad invocando la protección del interesado, por cuanto todas las personas gozarán, en cada uno de los países comunitarios, de una protección equivalente de alto nivel.

La Resolución de los representantes de los Estados miembros de las Comunidades Europeas, de 1990, hizo extensivos los principios de la Directiva a los ficheros del sector público no incluidos en su ámbito de aplicación, tales como los de las administraciones cuyas actividades no estén sujetas al Derecho Comunitario.

La Comisión, en su Declaración de Septiembre de 1990 manifestó el deseo de que los principios de la Directiva se aplicaran a las instituciones y organismos de la Comunidad, estableciendo la adopción de las medidas necesarias para la consecución de tales objetivos.

2. Directiva del Consejo, de 24 de Septiembre de 1990, relativa a la protección de datos personales y de la intimidad en el contexto de las redes digitales públicas de telecomunicaciones y, en particular, de la red digital de servicios integrados y de las redes digitales móviles públicas.

Esta Directiva aplica los principios generales de la protección de datos a las necesidades específicas de los nuevos sistemas de telecomunicación.

Su objetivo es garantizar a los usuarios de las redes de telecomunicaciones de los Estados miembros un nivel básico de protección, a través de medidas que deben integrarse en los servicios ofrecidos por las nuevas redes.

c) Seguridad de la Información:

1. Decisión del Consejo relativa a la adopción de un plan de acción en materia de seguridad de los sistemas de información.

La seguridad de la información (protección de datos conservados, tratados y transmitidos electrónicamente) contra todo tipo de amenazas es esencial para el ejercicio efectivo de los derechos de las personas en lo referente al tratamiento de datos personales. La seguridad constituye un requisito imprescible para la protección de personas y bienes que hacen necesarios el desarrollo de una política común, de medidas consensuadas en el campo tecnológico

y de los procesos de homologación, y en definitiva del perfeccionamiento de tecnologías, que constituye un pilar básico sobre el que fundamentar la realización del Mercado Unico.

2. Reglamento del Consejo, de 1992, relativo a las medidas de seguridad aplicables a las informaciones clasificadas elaboradas o intercambia– das en el marco de las actividades de la CEE y de la CEEA.

Define el marco que permitirá el intercambio de las informaciones clasificadas, en la medida necesaria, entre las instituciones y entre éstas y los Estados Miembros.

Se trata de un reglamento de carácter técnico en el que se establecen las normas y los principios básicos que regulan las condiciones de intercambios de informaciones clasificadas, y las medidas de protección de que serán objeto dichas informaciones durante su elaboración, circulación y conservación. No pretende contravenir el principio de publicidad de las informaciones, ni interferir en la libertad de las instituciones y los Estados Miembros para establecer el nivel de clasificación de una información, siempre que se respete mutuamente la clasificación que se decida. El Reglamento, por último, señala también que la clasificación de una información sólo debe realizarse cuando estén en juego intereses fundamentales y por el tiempo que sea necesario.

B. Equivalencia de la protección comunitaria: Nivel interior y Nivel exterior.

Para garantizar la protección de todas las personas residentes en la Comunidad en lo referente al tratamiento de datos personales es necesario establecer un nivel de protección equivalente para toda la Comunidad.

El artículo 100 A del Tratado proporciona la base jurídica necesaria, por cuanto es indispensable una protección equivalente de alto nivel para la realización del mercado interior; definido éste en el artículo 8 A como «espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones del presente Tratado». Su funcionamiento hace necesario un acercamiento de las legislaciones en este campo.

Para conseguir esta aproximación, resulta necesario el establecimiento de un doble campo de actuación:

1. Nivel Interior.

Aparte de las medidas legislativas adoptadas, a las que nos hemos referido anteriormente, es necesario por parte de los Estados Miembros, la creación de una legislación nacional, o bien la modificación o supresión de las disposiciones legislativas, reglamentarias o administrativas existentes, (en aquellos que la poseen) para adaptarlas a la política y a los objetivos comunes elaborados por las instituciones comunitarias. Sólo así se podrá llevar a buen

puerto la voluntad de enlazar la esencial unidad, manteniendo la variedad de particularidades nacionales.

Los Estados Miembros, sus instituciones y autoridades están obligados directamente por el derecho comunitario y deben respetarlo como si se tratara de derecho nacional; pues como reiteradamente ha señalado la jurisprudencia comunitaria, al igual que las leyes nacionales confieren derechos o imponen obligaciones a los ciudadanos comunitarios.

La problemática de las bases de datos no debe ser ajena a este razonamiento sino todo lo contrario. El establecimiento de medidas comunitarias de protección debe constituir, a la vez que un marco común de referencia para los Estados Miembros, la base sobre la que debe asentarse en el futuro el desarrollo de medidas legislativas sobre la materia. Sólo así se conseguirá una efectiva igualdad entre los ciudadanos comunitarios, tanto en la titularidad de los derechos, como en el ejercicio de las garantías que le asisten para la efectividad de los mismos.

2. Nivel Exterior.

La Comunidad Europea debe promover en los foros en que participa la aplicación de disposiciones adecuadas y apoyar los esfuerzos emprendidos por el Consejo de Europa en la materia. Estas propuestas no pueden separarse entre sí, sin poner en peligro la homogeneidad y coherencia del sistema comunitario propuesto.

Teniendo en cuenta que los actuales sistemas de comunicación permiten el flujo de datos a nivel mundial, las medidas y actuaciones comunitarias deben tener en cuenta este dato, para abordar el problema desde una concepción global que comprenda, no sólo su ámbito territorial de actuación, sino también la de aquellos con los que se relacionan, a través de propuestas de creación de bases de datos conjuntas, transferencias tecnológicas y acceso a los sistemas de información.

La Comunidad Europea ante la Circulación de datos personales. Su protección jurídica

M.ª DEL CARMEN TIRADO ROBLES
Licenciada en Derecho
(ESPAÑA)

SUMARIO

INTRODUCCION
TRATAMIENTO DEL TEMA A NIVEL INTERNACIONAL
La Comunidad Europea
Recomendaciones del Parlamento europeo
El proyecto de Directiva de 1990
EL SIS EN EL ACUERDO SCHENGEN
CONSIDERACIONES FINALES

INTRODUCCION

La protección de datos personales constituye hoy un importante criterio de legitimación política de los sistemas democráticos tecnológicamente desarrollados. Su reconocimiento es condición necesaria para el funcionamiento del sistema democrático, es una garantía básica para cualquier comunidad de ciudadanos libres e iguales. La protección de datos personales y las libertades en relación con el uso de la informática han pasado a formar parte del conjunto de los derechos que, según E. DENNINGER «definen el status constituens del ciudadano, su posición jurídica de formar parte activa y constituyente del Estado»[1].

[1] PÉREZ LUÑO, A. E., «Libertad informática y derecho a la autodeterminación informa-

La protección de datos en nuestros días hace referencia al conjunto de bienes o intereses que pueden ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables. O, según G. GARZÓN CLARIANA «el derecho individual a la protección de datos se reconoce como un derecho a un uso de la informática respetuoso para con los intereses protegibles de la persona sobre los datos que le conciernen y controlado por los poderes públicos»[2].

Este derecho aparece normalmente desarrollado en los ordenamientos nacionales por medio de leyes ordinarias, y tutelado mediante órganos expresamente creados al efecto.

Toda esta legislación de carácter tuitivo, aunque necesaria, es insuficiente pues el avance tecnológico y las relaciones económicas confieren al problema una dimensión internacional.

TRATAMIENTO DEL TEMA A NIVEL INTERNACIONAL

Así como la protección de datos sólo es un aspecto dentro del régimen jurídico de las corrientes internacionales de datos, éstas no delimitan el ámbito en que se advierte como imprescindible la cooperación internacional para la tutela de los datos personales[3].

Una disparidad demasiado marcada entre los niveles de protección garantizados por los derechos internos tendría efectos negativos, por ejemplo, el traslado del tratamiento informático de datos personales al territorio de los Estados con reglamentación menos exigente, marginación de empresas de estos mismos Estados por parte de agentes económicos de otros menos escrupulosos..., las consecuencias serían más graves en la hipótesis de que los Estados formasen parte de una misma organización de integración económica.

DÍEZ DE VELASCO [4] opina que esta materia tiene un gran interés en el aspecto internacional y, dada la magnitud de los intereses en juego, sólo puede ser tratada adecuadamente mediante la cooperación entre Estados. La legislación interna de cada país puede entorpecer las corrientes de circulación de datos a través de las fronteras, frenando el comercio internacional de servicios informáticos o bien introducir diferencias acusadas en los requisitos de seguridad técnica forzando a las multinacionales del sector a la diversificación de los modelos de ordenador, lo que tendría efectos catastróficos para los costes de producción de estas empresas.

---

tiva», Congreso sobre Derecho informático de Zaragoza, Textos de ponencias y comunicaciones, edición previa, 715 pp., 1989 p. 359.

[2] GARZÓN CLARIANA, G., «La protección de datos personales y la función normativa del Consejo de Europa», Revista de Instituciones Europeas, 1, 1981 p. 9-25.

[3] Ver nota 2.

[4] DÍEZ DE VELASCO, "Instituciones de Derecho Internacional Público», Madrid, Tecnos, 1988, p. 186.

La propia práctica demuestra que se ha producido una constante interacción entre la preparación de leyes internas y tratados internacionales.

La preocupación internacional por estos temas aparece ya a fines de los años 60 en la Conferencia Internacional de Teherán, en el seno de la ONU, pero es en el plano europeo y atlántico donde las realizaciones son de mayor importancia ya que en este ámbito se encuadran los países más afectados por la irrupción de la informática: la OCDE aprueba el 23 de septiembre de 1980 una Recomendación relativa a «las directrices aplicables a la proteccción de la vida privada y a los flujos transfronteras de datos personales» que tiene principios prácticamente idénticos a los que luego se recogen en el Convenio del Consejo de Europa del que más tarde hablaremos; el texto de la Recomendación no es obligatorio, pero se reconoce su importancia en las empresas transnacionales al haber encarecido su observancia las últimas administraciones norteamericanas.

Es en el Consejo de Europa donde nacen las iniciativas más relevantes: en 1969 la Asamblea Parlamentaria debate el artículo 8 del Convenio Europeo sobre Derechos Humanos y llega a la conclusión de que es necesaria una regulación de las condiciones en que las informaciones relativas a los individuos identificables podrían ser recogidas, utilizadas y transmitidas parcialmente al extranjero. El logro final fue «inventar» la protección de datos propiamente dicha[5].

El Consejo de Ministros del Consejo de Europa adopta en 1973 y 1974 sendas Resoluciones sobre la protección de la vida privada de los individuos, con respecto a los bancos de datos electrónicos[6].

Después, en el año 1981, el Consejo de Europa aprueba el Convenio para la protección de las personas con respecto al tratamiento informatizado de datos de carácter personal, con un ámbito de aplicación más amplio de lo que en principio podría pensarse, ya que según el artículo 24 los Estados miembros pueden extender su aplicación a otras áreas geográficas, y según el artículo 23 el Comité de Ministros puede invitar a otros Estados a adherirse al Convenio.

Con la elaboración de este Convenio se produce un considerable avance en las legislaciones nacionales, que reciben un impulso en esta materia. Es el único Tratado multilateral sobre la materia hasta el momento y abre una perspectiva de colaboración internacional a nivel europeo occidental en el preocupante terreno de la protección de datos personales.

---

[5] LÓPEZ MAYOR, V. «La legislación informática en el ordenamiento jurídico español». Congreso sobre Derecho Informático de Zaragoza, textos de ponencias y comunicaciones, edición previa, 715 pp., 1989, p. 415.

[6] Para el sector privado la resolución 22/73 y para el sector público la resolución 29/74.

La Comunidad Europea.

La Comunidad Europea inicia el camino con una Resolución del Parlamento europeo sobre protección de los derechos de la persona, cuyo objeto es invitar a la Comisión a preparar una propuesta de Directiva con el fin de armonizar las legislaciones nacionales en materia de protección de datos a un nivel que ofrezca el máximo de garantías a los ciudadanos comunitarios; por otra parte, el mismo Parlamento pide a la Comisión y al Consejo que, en la elaboración de normas jurídicas, tenga en cuenta sus recomendaciones, que avanzan principios que ya se encontraban en la ley francesa:[7] establecimiento de reglas sobre la colecta de datos, obligación de almacenar únicamente los datos exactos y necesarios para la finalidad del fichero, puesta en marcha, tanto a nivel comunitario como de cada Estado miembro, de organismos independientes de control ...

Recomendaciones del Parlamento europeo.

Por otra parte, el Parlamento Europeo [8] juzga que, los flujos transfronteras de datos personales provenientes de un Estado miembro y con destino a otro, no deben estar sometidos a ningún reglamento especial, sólo deben ser notificados al órgano de control de la Comunidad.

El proyecto de Directiva de 1990.

Al mismo tiempo que las autoridades comunitarias recomiendan a los Estados miembros adherirse a la Convención del Consejo de Europa[9], la Comisión propone la adopción de una Directiva «relativa a la protección de las personas con respecto al tratamiento de datos de carácter personal» que se presentó el 27 de julio de 1990.

Su objeto es establecer «una protección equivalente de alto nivel en todos los Estados miembros de la Comunidad Europea, a fin de eliminar los obstáculos a los intercambios de datos necesarios para el funcionamiento del Mercado Interior»[10].

Hará falta seguir la evolución de las cosas, la verosimil adopción de la Directiva antes citada, antes de reconsiderar las soluciones nacionales presentes que, por supuesto, se verán altamente afectadas. La opinión de la Comisión Nacional de Informática y Libertades (CNIL) francesa no es diferente, pues en su informe de 1990 hace una crítica severa del proyecto de instrumento comunitario en el cual ve un riesgo de debilitamiento del nivel de protección. Al mismo tiempo, igualmente sensibles al movimiento anunciado,

---

[7] Ley Francesa 78/17, de 6 de enero de 1978, relativa a la informática, los ficheros y las libertades, tradicionalmente denominada en Francia Ley «Informática y Libertades».

[8] SIEGLERSCHMIDT, M. Parlamento Europeo, Documentos de sesiones, Doc. 1–548/81, de 12 de octubre de 1981 y D.O.C.E de 5 de junio de 1979, serie C, 140 p. 34 y 37.

[9] Recomendación de la Comisión de 29 de julio de 1981 y Recomendación del Consejo de 13 de septiembre de 1990.

[10] Publicada en D.O.C.E., serie C, 5 de noviembre de 1990, n.º 227, p. 3 a 12.

los representantes de los diversos sectores económicos se reparten curiosamente entre la adhesión a una fórmula en la que ven un alivio a los apremios que pesan sobre ellos y la creencia de estar sometidos a reglas nuevas.

Dejando de lado toda polémica, lo cierto es que el proyecto se aparta mucho en ciertos puntos de la filosofía que rige el Derecho positivo francés[11].

En cuanto al contenido propiamente dicho del proyecto de Directiva, se ha de decir que tanto éste como el Convenio del Consejo de Europa tienen el mismo objeto: la protección de la intimidad o vida privada respecto al tratamiento automatizado de datos personales. Pero además, la propuesta comunitaria incluye la libre circulación de datos personales, con lo que parece seguir la tendencia de la Comunidad de llegar a la integración total (tanto económica como política) por medio de las cuatro libertades básicas del sistema comunitario, integrando entre ellas la libre circulación de datos automatizados.

Por otra parte, la propuesta incluye definiciones de términos especializados, a veces distintos de los del Convenio del Consejo de Europa, pero la propuesta de Directiva es más amplia ya desde su concepción pues, como la misma indica en su considerando 22, se va a ocupar de concretar y ampliar el Convenio del Consejo de Europa.

Se incluyen principios como el de información a las personas interesadas, la necesidad del consentimiento de éstas, el derecho de acceso, el de rectificación, el principio de pertinencia de los datos... En lo que se refiere a los flujos transfronteras de datos, la regla es que el país receptor asegura «un nivel de protección adecuada», a falta de lo cual la Comisión entablará negociaciones con dicho país para solucionar esta situación, o bien el país miembro puede autorizar la operación si el responsable del fichero está dispuesto a garantizar un nivel de protección adecuada y los otros Estados no se oponen en los diez días siguientes.[12]

Ahora esta propuesta está en fase de modificación en el seno de la Comisión. Habrá que esperar a su adopción para analizar cómo se configura el sistema finalmente. Lo que sí es cierto es que su influencia en las legislaciones europeas será importante, pues éstas deberán modificarse, si no lo han hecho ya, en el sentido que indique la Directiva. Además el proyecto indica un plazo máximo a los Estados miembros para su transposición (como todas las Directivas) que se fija en el 1 de enero de 1993.

---

[11] VIVANT, M. y otros. «Une proposition de directive communaitaire», Droit de l'Informatique. LAMY S.A., París, 1992, n.º 1157, p. 709.

[12] VIVANT, M. y otros. «Les initiatives communautaires: la résolution et la recommandation du Parlament européen de 1979, le provet de directive de 1990», Droit de l'Informatique. LAMY S.A., París, 1992, n.º 1713, p. 1080.

EL SIS EN EL ACUERDO DE SCHENGEN

Bélgica, Francia, Luxemburgo, Países Bajos y la antigua República Federal Alemana firmaron el 14 de junio de 1985 en Schengen un acuerdo que se presentaba como «laboratorio de la Europa de 1993».[13]

Se centra especialmente en la supresión de todo control en las fronteras comunes, transfiriéndolo a las fronteras exteriores. Al mismo tiempo y para hacer frente al déficit de seguridad surgido por esta apertura de fronteras, se prevé un reforzamiento de la cooperación policial entre los países miembros mediante un sistema de información automatizado común que centraliza las informaciones que las policías nacionales se intercambian ya bilateralmente.

El Systeme d'Information Schengen (SIS) comporta que las informaciones calificadas por algunos Estados como «muy sensibles» servirán, no sólo para señalar a personas sospechosas, sino también para buscar a personas desaparecidas, recoger de manera más o menos secreta informaciones en todos los ámbitos, rechazar o extraditar extranjeros indeseables y efectuar controles aduaneros fuera de las fronteras.

Las instancias nacionales de control del uso de los datos nominativos admitieron que la armonización de la protección se hiciera al nivel resultante de la combinación de las disposiciones de la ley francesa de 6 de enero de 1978 [14] y las del Convenio del Consejo de Europa de 20 de enero de 1981.

Los representantes de estas autoridades, reunidos el 17 de marzo de 1989 en Luxemburgo, adoptaron una declaración que prevé que la puesta en marcha del SIS estará subordinada a las siguientes directrices: [15]

–la definición precisa y definitiva del contenido del fichero;

–la existencia de un derecho de acceso, de rectificación de las informaciones y de supresión de las no pertinentes;

–la habilitación, en cada país, de una instancia de control independiente;

–la creación de un órgano común de estudio y armonización, compuesto de representantes de los órganos nacionales de control;

–la asociación de los órganos de control ya existentes para la elaboración del SIS;

–la toma en consideración de las disposiciones del Convenio del Consejo de Europa para la protección de las personas al respecto del tratamiento automatizado de datos personales, como obligaciones mínimas.

---

[13] FONTAINE, P. «La Europa de los ciudadanos», colección Europa en movimiento. Comisión de las Comunidades Europeas, Bruxelas, 1991.

[14] Ley «Informática y Libertades» antes citada.

[15] VIVANT, M. y otros. «L'Accord de Schengen sur la supresion des contróles aux frontiéres», Droit de l'Informatique. LAMY S.A., París, 1992, n.º 1715, p. 1081.

El 19 de junio de 1990 se firma el Convenio de aplicación de este acuerdo, que pone en marcha un sistema de intercambio de datos informatizados. Concierne a los extranjeros a quienes se les ha rechazado su entrada en el país por razones de orden público, personas implicadas en gran criminalidad, personas buscadas en el cuadro de un procedimiento judicial, las desaparecidas, los menores huidos...

El texto afirma la obligación de los países signatarios de tomar todas las disposiciones para asegurar un nivel de protección equivalente a los principios del Consejo de Europa.

Se prevé además, en los artículos 37 y 38 del Convenio de aplicación, la creación de un fichero propio de los demandantes de asilo distinto al SIS. Las informaciones recogidas comprenden especialmente la identidad del interesado, la naturaleza de los documentos de identidad y viaje, los lugares de estancia y el itinerario seguido, el lugar de depósito de la demanda de asilo, la fecha de una eventual demanda anterior, el estado del procedimiento de examen y, en su caso, el contenido de la decisión tomada. Si el interesado consiente, puede ser suministrada de Estado a Estado la información sobre los motivos invocados en la demanda de asilo y los motivos de la decisión tomada.[16]

Este fichero de demandantes de asilo comporta un peligro de difusión entre los Estados de los datos que conciernen directamente a los derechos de las personas, ya que son datos de carácter étnico, político, religioso... y según el Convenio de Ginebra el itinerario seguido puede incluir países en los que la seguridad del demandante de asilo no está plenamente asegurada en caso de que fuera objeto de reenvío.

CONSIDERACIONES FINALES

La Comunidad Europea se ha ocupado de la materia de protección de datos personales desde diversos ámbitos y hace ya cierto tiempo, si bien es verdad que el hito más importante en este camino, la propuesta de Directiva de 1990, no es aún legislación comunitaria en vigor. Aún así, existe en la Comunidad un Grupo de protección de datos personales, al igual que en el Consejo de Europa existe un Comité Consultivo sobre la misma materia.

Pensamos por ello que el Derecho Comunitario debe ser tenido en cuenta en los Estados miembros pero también en el resto de los países con un uso de la informática desarrollado, ya que las soluciones en Europa pueden ser modelo para otros.

---

[16] JULIEN–LAFERRIERE, F. «Le droit d'asile et la Convention de Schengen», L'Europe des polices et de la sécurite intérieure. Dirección de BIGO, D. ED. COMPLEXE, Bruselas, 1992, p. 129.

Otra cuestión es decidir si el tema se encuadra dentro de la libre circulación de mercancías o de servicios. [17]

Por otra parte, habrá que tener en cuenta los problemas que surgirán al chocar las legislaciones internas de los Estados miembros con la legislación comunitaria en creación, propios del Derecho Internacional Privado.

Son todas ellas cuestiones que merecen ser seguidas en el futuro, cuando la legislación hoy en elaboración, esté ya en vigor.

BIBLIOGRAFIA

DIEZ DE VELASCO, «Instituciones de Derecho Internacional Público», Madrid, Tecnos, 1988, p. 186.

FONTAINE, P. «La Europa de los ciudadanos», colección Europa en movimiento. Comisión de las Comunidades Europeas, Bruselas, 1991.

GARZON CLARIANA, G., «La protección de datos personales y la función normativa del Consejo de Europa», Revista de Instituciones Europeas, 1, 1981, p. 9-25.

JULIEN-LAFERRIERE, F. «Le droit d'asile et la Convention de Schengen», L'Europe des polices et de la sécurite intérieure. Dirección de BIGO, D. Ed. COMPLEXE, Bruselas, 1992, p. 129.

LOPEZ MAYOR, V. «La legislación informática en el ordenamiento jurídico español». Congreso sobre Derecho Informático de Zaragoza. Textos de ponencias y comunicaciones, edición previa, 715 pp., 1989 , p. 415.

PEREZ LUÑO, A.E., «Libertad informática y derecho a la autodeterminación informativa», Congreso sobre Derecho informático de Zaragoza. Textos de ponencias y comunicaciones, edición previa, 715 pp., 1989, p. 359.

SIEGLERSCHMIDT, M. Parlamento europeo, Documentos de sesiones, Doc. 1-548/81, de 12 de octubre de 1981 y D.O.C.E. de 5 de junio de 1979, serie C, 140 p. 34 y 37.

VIVANT, M. y otros. «Une proposition de directive communautaire», Droit de l'informatique. LAMY S.A., París, 1992, nº 1157, p. 709.

VIVANT, M. y otros. «Les initiatives communautaires: la résolution et la recommandation du Parlement européen de 1979, le proyet de directive de 1990», Droit de l'informatique. LAMY S.A., París, 1992, nº 1713, p. 1080.

VIVANT, M. y otros. «L'Accord de Schengen sur la supression des contrôles aux frontières», Droit de l'informatique. LAMY S.A., París, 1992, nº 1715, p. 1081.

[17] Sobre esta polémica, en la que no voy a entrar, ver la exposición que recoge VIVANT, M. y otros: «Explotation de l'existant en droit communautaire», Droit de la l'informatique. LAMY S.A., París, 1992, n.º 1751 a 1758, p. 1104 y ss.

VIVANT, M. y otros. «Explotation de l'existant en droit communautaire», Droit de l'informatique. LAMY S.A., París, 1992, nº 1751 a 1758, p. 1104 y ss.

COLOQUIOS

PREGUNTA: La pregunta en específico es si de los temas del Proyecto, de la LORTAD nos van a dar copia a todos y cada uno de los delegados, ántes de que publique el Congreso sus actas.

RESPUESTA DE D. RAFAEL GONZALEZ-TABLAS. COORDINADOR: Se pueden dar los datos, porque ahora está en trámite en el Senado y, posiblemente, sufrirá o no modificaciones en función de ello. No sé hasta qué punto conviene invertir dinero en que se lo lleven Vds., pero, en principio, en el Boletín Oficial de las Cortes Generales, Congreso de los Diputados, en la IV Legislatura, en la serie a), Proyectos de Ley de 25 de Mayo de 1992, es el número 59, el correlativo 11. El correlativo 1 se corresponde al 59.1 que es el Proyecto de Ley inicial. El correlativo 11 es el que se corresponde con la aprobación por el Pleno del Senado, y los correlativos siguientes, se corresponderán con los Trámites de la Comisión del Senado, el resultado del dictámen de la Ponencia del Senado y luego el Pleno del Senado. Caso de que hubiese modificaciones, pasaría al trámite correspondiente de la Comisión Mixta Congreso-Senado, y, por último, pasaría a publicación en el Boletín Oficial del Estado (BOE), que entonces sería cuando se constituiría en Ley, es decir, que todavía queda tiempo.

SIGUE LA PREGUNTA: Tal vez la pregunta es con relación a ambos, uno que es un Proyecto de Ley, y otro que es ya una Ley en Portugal.

RESPUESTA: La ley portuguesa yo no la he traido, pero la Profesora Castillo es posible que sí, puede facilitarla a la Organización, y si esta tiene los medios, que haga la reproducción pertinente.

PREGUNTA: La diferencia entre los perfiles estadísticos y psicológicos, si se puede establecer claramente -como para los perfiles estadísticos-, que se pueda conocer que determinada persona va a determinado restaurante tantas veces por semana ¿Ese es un perfil más estadístico que de la persona?

RESPUESTA DE D. ANTONIO PEREZ LUÑO: Bien, en materia de Protección de Datos, a veces nos encontramos con que se da esa famosa Ley de la Dialéctica, del paso de la cantidad a la cualidad. A veces un perfil

meramente estadístico, es lo suficientemente revelador como para convertirse en un perfil sobre la personalidad de un sujeto. Cuando una persona viaja desde Sevilla a Madrid en una determinada ocasión, eso no tiene la mayor importancia; si se ve que periódicamente, en los mismosdías de la semana y a las mismas horas viaja, entonces eso puede dar lugar, junto, por supuesto, con otros datos, a que de ahí se extraigan consecuencias que son peligrosas para su personalidad. Del mismo modo, hubo un tiempo en las Leyes de Datos de la llamada Segunda Generación de Leyes de Protección de Datos, en torno a la década de los años 70, donde se consideraba que la protección más importante en materia de datos personales, era la definición de qué datos eran sensibles, y qué datos no lo eran, y hoy algunos tratadistas, e incluso algún movimiento de la propia Jurisprudencia en algunos países, concretamente en Italia y en Alemania, tienden a relativizar los datos sensibles de los que no lo son, porque cualquier dato, que en principio no tiene importancia, puede ser sensible, a tenor del uso que se haga de él. Un dato irrelevante, un dato como puede ser lo que me está recordando el Profesor González-Tablas, los cuartos de baño que tiene una persona, y que venían en la Ley del Censo, y que cada uno tenía que decirlo; eso es un dato irrelevante, pero luego, sobre él se pueden hacer determinadas lecturas y sacar unas determinadas consecuencias de tipo político, económico, etc., sobre esos datos. O sea, que volviendo a lo que Vd. me dice, un dato puramente estadístico y cuantitativo puede, según la utilización que se haga de él, convertirse en un dato agresivo para la intimidad o para los derechos fundamentales de una persona. Por eso hoy se tiende más, en las leyes de la llamada Tercera Generación de Protección de Datos, del año 80 en adelante, en establecer el sistema de garantías en base a la utilización que se haga del dato personal, más que en la definición de calidades de datos, aunque, evidentemente, siempre en esto la LORTAD mantiene el principio del Convenio Europeo, etc., de que hay determinado tipo de informaciones que se refieren a creencias religiosas, creencias ideológicas, datos sanitarios, etc., que se considera que tienen más relevancia que otros, efectivamente puede ser así. Pero ya digo, un dato en principio irrelevante, puede serlo a tenor de la utilización que de él se haga.

PREGUNTA: Yo quería comentar que, si en definitiva no tenemos la impresión –con lo que estamos tratando esta tarde, y el tema genérico que será la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos, en realidad el tema de este Congreso– de que últimamente en este estado Democrático de Derecho, hay una profusión legislativa, y que tristemente, en todas las nuevas leyes que se están creando, Leyes Orgánicas sobre Derechos Fundamentales, siempre encontramos en esta hasta que nos tenemos que defender frente a la ley. Es que es algo triste que una ley, desde el mismo momento en que sale, nos estemos planteando que nos tenemos que defender frente a lo que nuestro legislador hace. Propiamente lo que tendríamos que

preguntarnos es ¿quién hace las leyes? ¿las leyes las hace realmente el Parlamento que es el representante del pueblo español, o quizá es que sólo la haga una pequeña comisión que es el Gobierno, y quiza no entero, y luego la disciplina de partido impone qué hay que decir que sí?, porque es que como ésta, tenemos la Ley Orgánica de Protección de la Seguridad ciudadana, realmente bochornosa, que hay juristas de relevancia, que saben lo que están diciendo, que hacen una crítica atroz. Esta ley y otras leyes que últimamente ponen en tela de juicio la misma esencia del Estado de Derecho, Principio de Seguridad Jurídica, Principio de Libertad, que es uno de los valores esenciales de nuestro ordenamiento jurídico. Yo estoy realmente alarmada.

Ciñéndome, la pregunta es ¿Qué impresión les merece la LORTAD? Puesto que nos tenemos que defender frente a ella, rogaría a la Profesora M.ª EUGENIA GAYO SANTA CECILIA me comentara qué opinión tiene.

RESPUESTA DE DÑA. M.ª EUGENIA GAYO: Voy a intentar decirle algo de lo que ya he dicho. Mi impresión es altamente negativa, por lo menos en el ámbito de las garantías, es decir, para mí la ley viene a mermar sensiblemente el sistema de garantías que nuestra propia Constitución ya nos había dado en materia de derechos fundamentales, y, lógicamente, eso me pone en alerta. Yo poco más puedo hacer, mas que quizá utilizar esta Tribuna u otras para poner también el alerta a los demás, y que puedan empezar a pensar en posibles vías de defensa ante la propia ley. Yo no hago la ley, y en ese sentido, quizá tiene Vd. razón en que puede haber problemas en el ámbito parlamentario que deriven y conduzcan a esta situación. La realidad es que estamos ante un Proyecto que supuestamente en breve plazo, se tramitará por el Senado y se publicará en el Boletín Oficial, de manera que será ya la Ley Orgánica, y que tiene lo que tiene. Ante ella, la contestación que le doy es la que le he dado ántes. Yo pretendo encontrar, si el texto no se modifica, algún sistema para protegerme frente a la propia ley, ya que la ley me está mermando el sistema de protección que yo ya tenía.

INTERVENCION DEL D. ANTONIO ENRIQUE PEREZ LUÑO. COORDINADOR DE SESION: Muchas gracias. Al objeto de que nadie piense que estoy aquí como convidado de piedra, voy a intentar reconducir lo que puede ser el debate de las interesantísimas comunicaciones que acabamos de escuchar.

Sin entrar en lo que pueden ser preguntas puntuales a cada una de las intervenciones, que yo creo que va ha haberlas, yo querría establecer unos parámetros generales, si se quiere unos bloques temáticos de las cuestiones de base que se han suscitado por debajo de estas consideraciones comparatistas e internacionalistas sobre el tema de la Protección de Datos Personales.

PRIMERA REFLEXION: Las necesidades de tipo antropológico individual y colectivo, los valores éticos y jurídicos, los peligros de agresión a esos valores y a esas necesidades son comunes, son compartidos por grandes sectores de la humanidad actual, pero, sin embargo, la respuesta normativa no es unívoca. Vemos que todavía quedan grandes sectores de países, grandes bloques de países que no han dado una respuesta normativa a estas importantes necesidades, valores y peligros. Y vemos que aquellos que la han dado, han dado una respuesta que no es del todo igual, que no es homogénea, y esto es un primer punto de reflexión, el interrogarse por qué esto sucede, y cuáles pueden ser los medios para superarlo.

SEGUNDA REFLEXION: Parece, y se ha desprendido un poco de las intervenciones que hasta aquí acabamos de escuchar, que por el momento, son las Organizaciones Internacionales de tipo regional, como es la Comunidad Económica Europea, las que estan avanzado de forma más positiva, más provechosa, en este ámbito, en el ámbito de dar unas directríces comunes para la protección de los datos personales, pero, sin embargo, aquí también se ve la tensión contínua entre la necesidad, o si se quiere, la ambición de esas comunidades, de esas organizaciones regionales o esas organizaciones internacionales, de dar pautas comunes de reglamentación normativa, y todavía la pretensión de los Estados de defender (los Estados miembros de las organizaciones) su soberania legislativa y de poner trabas a una posible inje-

rencia, de lo que consideran una injerencia excesiva en sus competencias de soberanía legislativa interna.

TERCERA REFLEXION: Que, por supuesto, la acción normativa de las organizaciones internacionales regionales, siendo muy positiva, siendo muy provechosa, siendo en estos momentos el camino a seguir, pero no es suficiente. ¿Por qué? Pues porque, aludiendo a un tema que se ha planteado esta mañana, de los llamados derechos humanos de la Tercera Generación, lo que caracteriza a los valores, las necesidades que se debaten debajo de esos derechos, o los peligros que acechan bajo la necesidad de proteger esas situaciones, es que son derechos sin fronteras. En cuanto limitemos a un ámbito territorial la protección de esas facultades, hemos perdido la batalla por la defensa y la garantía de esos derechos, y entonces ¿de qué me sirve a mí, incluso pertenecer a una Comunidad como la Comunidad Europea, donde parece que somos privilegiados en las pautas jurisdiccionales de defensa jurídica? (basta pensar en la Comisión y el Tribunal de Estrasburgo, etc., si incluso muchos de mis datos personales si no existen reglas a nivel internacional general, pueden estar en estos modementos codificados, elaborados, etc, en bancos de datos que están en Estados Unidos, a través de las tarjetas de crédito, pongo por caso.

¿Qué quiere decir? Que la batalla por la protección de los datos personales, desde luego no se puede interpretar jamás, no se puede alcanzar jamás un resultado positivo, si se quiere lograr todo en un momento, sin pasos previos. Todas las conquistas históricas han sido conquistas paulatinas, pero que no debemos pensar, no debemos tener esa mentalidad un poco egoísta de porque pertenecemos a un Estado que en un determinado momento tenga normas de protección de datos, o a una Comunidad internacional regional que las tenga, ya, todos los problemas han sido solventados, porque, repito, en los problemas de los derechos humanos de la Tercera Generación, no existen fronteras, y entonces, si no existe una protección internacional, general, global, total, o como se quiera llamar, nunca podremos estar del todo seguros, o del todo tranquilos.

CUARTA REFLEXION: Las normas sobre datos personales, sobre transmisión de informaciones, etc., utilizando la distinción clásica de Norberto Bobbio, no se deben considerar sólo como normas de tipo represivo, deben ser también normas promocionales, es decir, evidentemente, el flujo incontrolado de informaciones representa un riesgo para determinados derechos. Pero es que vivimos en una sociedad donde la información significa progreso, donde el flujo de las informaciones en todos los estadios, en el terreno técnico, en el terreno científico, en el terreno de la cultura, también en el terreno sanitario, en todos los aspectos, es fundamental para el progreso, y entonces yo pienso que hay que establecer una legislación equilibrada en las normas y

en las pautas internacionales de protección de datos, que evitando los paraísos informáticos, evitando los lugares donde exista una especie de «patente de corso» para utilizar informaciones personales, pero que tampoco sea tan restrictiva, y eso tiende en algunos convenios de tipo internacional, que impida ese progreso que representa el flujo de informaciones, hasta cierto punto, si en el orden interno se dice que no hay una sociedad democrática donde no exista intercambio de informaciones, también en el orden internacional, la sociedad internacional no podrá ser libre y democrática, allí donde no exista una equilibrada difusión de informaciones.

Con esto, creo que podemos empezar el debate.

PREGUNTA: Es una pregunta dirigida a toda la Mesa. Yo vengo de América, de México. En ese lugar no nos planteamos tanto la Protección de Datos Personales en este momento, y después de escuchar todas sus intervenciones me queda una duda, y veo que puede existir un peligro al equiparar a los entes públicos con los entes particulares. El hecho de darle facultad a una agencia de información, de revisar las bases de datos a los particulares, y que estos tengan que informar, pudiera ser que estos particulares se inhiban de generar las Bases de Datos que les hacen falta. Se mencionó un ejemplo: Cuando tenemos necesidad de una base de datos de morosos. Pensemos en los abogados: todos los abogados necesitamos una base de datos de control y de gestión de nuestros asuntos. Nada más claro de tener ahí datos personales de nuestros clientes. Esta oficina ¿va a ir también a revisar esas bases de datos? ¿Estos abogados tendrán obligación de informarlos? ¿No se estará violando un derecho de los abogados, de una libertad profesional? ¿No se estará violando, por ejemplo, derechos como es la libertad de información? Si yo tengo información de morosos es porque yo la adquirí, y esa ya es propia, ya es mía. Si yo tengo esa información de particulares yo la debo proteger, hay una obligación de secreto profesional ¿No estarán perdiendo a lo mejor más de lo que se gane si se plantea eso?

RESPUESTA DE D. ETIENNE MONTERO: Creo que esto se contesta fácilmente, porque es verdad que muchas profesiones, muchos profesionales, tendrán que informar cuando tienen un banco de datos, pero hay el principio de finalidad, y si la finalidad expuesta es legítima, pues no habrá problemas; el fichero estará autorizado.

PREGUNTA: Quería decir respecto a la intervención anterior, porque viene al hilo, que todo depende del punto de vista desde el que uno se sitúe en esta vida. Todo depende de la forma de entender la vida y la sociedad, si uno está de acuerdo o no, si Vd. es partidario de que son prioritarios los intereses económicos de la abogacía, y yo soy licenciado en Derecho, pues eso sí es correcto. Ahora bien, si Vd. se sitúa desde un punto de vista de derechos fundamentales, eso no es así, porque es prioritario desde ese punto

de vista para una persona que sea demócrata y partidaria de los principios y derechos fundamentales, es prioritario defender el derecho a la intimidad y el derecho a que una persona de menos medios pueda acceder a un abogado para que, por ejemplo, al pobre no lo sigan engañando. Puede darse el caso perfectamente.

Una pregunta para el Sr. Montero. Dice Vd. que la Comunidad Económica Europea tiene la legislación más avanzada ahora mismo ¿no? , pero nos encontramos, sin embargo, que la Comunidad Económica Europea dice que el fin de la legislación existente, es eliminar los obstáculos al tráfico de datos automatizados para la mejor cooperación económica dentro de la Comunidad Económica Europea. Así, la legislación comunitaria no es, en principio, para la protección de derechos fundamentales, del derecho a la intimidad, sino para favorecer el desarrollo económico europeo, que, yo pienso que sí, que es muy positivo, que nos tenemos que unir en Europa, porque si no nos quedamos en el último vagón a nivel económico mundial, pero es más importante en estos países europeos occidentales avanzados la cuestión de los derechos fundamentales y de los derechos individuales. Si, en definitiva la Comunidad Económica Europea es el más avanzado y la Comunidad Europea lo primero que busca es eliminar obstáculos a una buena cooperación internacional, en realidad ¿qué legislación es entonces la que tiene como fundamento de ella misma, como la base, la búsqueda del respeto del Derecho Fundamental a la Intimidad y de todos los Derechos que de ella derivan en la informática?

RESPUESTA DE DÑA. M.ª DEL CARMEN TIRADO: La Comunidad Económica Europea sí que busca la cooperación, pero sólo entre los Estados miembros, porque es una organización internacional en ese sentido.

RESPUESTA DE D. SANTIAGO RIPOL: Me ha parecido entender la preocupación de quien formula la pregunta, y quizás sería conveniente explicar algunas cuestiones.

Se ha dicho que las organizaciones regionales eran donde más se desarrollaba o más desarrollado estaba, efectivamente, la normativa sobre Protección de Datos Personales.

En Europa occidental existen tres organizaciones que han trabajado un poco este sector: En primer lugar, la OCDE, que lo trabaja desde un punto de vista económico y estableciendo unas directrices que no son obligatorias para los Estados Miembros y es un texto de 1980 muy importante porque se recogen los principios que después los países tendrán que adoptar en su legislación interna.

En segundo lugar, el Consejo de Europa, que ha elaborado el único texto obligatorio a nivel internacional, que existe en el mundo, pero sólo tiene vigencia para los Estados de Europa Occidental que han ratificado este Convenio. España es uno de ellos. Y ahí se obliga primero a que los Estados parte del convenio elaboren una Norma sobre esto, una Ley de Protección de

Datos, y segundo, que esta Ley tenga los principios que se recogen en ese Convenio, que son, entre otros, el principio de libertad de acceso, el principio de que exista un órgano control diferencial entre datos sensibles y datos que no son sensibles, etc.

En tercero y último lugar, la Comunidad Europea, que se incorpora más tarde a esto. La Comunidad Europea ¿por qué regula la cuestión de los datos personales? Porque se lo encuentra en su objetivo esencial. La comunidad nació para crear un Mercado Común, en definitiva, para que entre España y Francia, por ejemplo, hubiera la misma relación en libertad de circulación de mercancías, etc., que entre Barcelona y Badajoz. Es decir, Sr. francés, yo he de tener las mismas posibilidades de que se vendan mis productos y los productos que yo elaboro en Barcelona, que el Sr. de Barcelona en Badajoz, y de ahí, las cuatro libertades: libertad de circulación de personas, libertad de circulación de trabajadores, etc.

Entonces, la Comunidad, el Tratado Constitutivo de la Comunidad no se preocupa para nada de los derechos fundamentales. Su objetivo es ese: construir un mercado común. Después de ha avanzado hacia un mercado único, pero no se preocupa para nada de los derechos fundamentales, entendido que ya existen en los países miembros de la comunidad unos principios que son compartidos y que se han recogido en un convenio del Consejo de Europa, la Convención Europea de Derechos Fundamentales de 1950, y cuando se encuentra la Comunidad en ese quehacer del Mercado Común, se encuentra la necesidad por ejemplo, de proteger la propiedad privada, o se encuentra la necesidad de proteger la intimidad, no se encuentra con una persona física, sino con una persona jurídica, y lo que hace es remitir a esos principios el Convenio de Roma de 1950. Creo que aquí ha pasado exactamente lo mismo. La Comunidad ha empezado a regular datos personales porque era esencial para la libre circulación de informaciones, es decir, para construir ese Mercado Común también es muy útil y es necesario que la información de un Banco de Datos en Barcelona pueda tenerla también el empresario alemán, y en esa volutad de construir ese Mercado Común, se ha encontrado con la Regulación de la Protección de los Datos Personales, como un límite, creo, a la libertad de información; y entonces lo que hace primero es remitir a los principios del Convenio del Consejo de Europa y decirle a los Estados miembros que regulen esas materias sobre la base de esos principios, y avanza un poco más en estas propuesta de directiva, para que los doce Estados miembros no tengan diferentes legislaciones, para homogeneizar un poco el nivel legislativo y que haya una protección similar.

SIGUE LA PREGUNTA: La pregunta era que qué les parecía que este texto, que precisamente busca, como bien ha dicho sólo favorecer el mejor desarrollo económico ¿Qué impresión nos da a nosotros, ciudadanos democráticos, que sea el más avanzado, el que lo único que busca es el mejor

desarrollo económico?. Entonces nosotros que tenemos la misma base de nuestro ordenamiento jurídico los derechos fundamentales y el derecho a la intimidad que es esencial, ¿qué nos parece eso?

RESPUESTA DE D. ETIENNE MONTERO: Se puede decir que ahí existe una organización en que se reflexiona fundamentalmente sobre estos temas, y es el Consejo de Europa. Es verdad que la Comunidad Económica tiene por objetivo hacer primero el Mercado Común, pero el Consejo de Europa, no. Tiene como objetivo reflexionar fundamentalmente sobre derechos humanos, sobre libertades fundamentales como esta libertad de la intimidad privada. Entonces, existe una organización a nivel europeo que reflexiona sobre estos temas y legisla también, con este Convenio de 1981.

SIGUE LA PREGUNTA: Yo hablaría que en todo en la vida existe interdisciplinariedad. Nadie puede olvidar un punto de vista político o ideológico a la hora de elaborar una ley. Una ley económica implica un punto de vista previo ideológico, de postura ante la vida o de postura ante el sistema o de lo que queramos, de principios básicos de cada ser humano. Y esto no se puede separar por más que Vds. pretendan situar a un lado lo económico y a otro lado estas cuestiones, que son la base de nuestro ordenamiento jurídico.

RESPUESTA DE D. ETIENNE MONTERO: Por eso la Comunidad Económica también se ha interesado en este tema de la Protección de la Vida Privada. No lo ha dejado sólo para el Consejo de Europa. También se ha interesado.

SIGUE LA PREGUNTA: Pero que están íntimamente imbricados. No podemos tratar una cosa sin tratar la otra.

RESPUESTA DE D. ETIENNE MONTERO: Sí. Cada organización tiene su misión específica, pero después la Comunidad Económica también se inspira en los trabajos del Consejo de Europa en estos aspectos.

PREGUNTA: Mi pregunta va dirigida al Profesor Francisco Eugenio. Vd. mencionó en su ponencia, en cuanto a los ficheros en bases de datos particulares, la necesidad de una autorización, una notificación por parte de la persona cuyo nombre se iba a incluir en el fichero. En mi país, Costa Rica, como en otros países de América, realmente todavía no existe una legislación acerca de los ficheros en bases de datos particulares. Mi pregunta es sobre la celeridad que debe existir en cuanto a la notificación o bien la autorización. La autorización es, para mi criterio, un trámite un poco más complicado que la notificación, porque la notificación implica únicamente la comunicación a la persona, mientras que la autorización necesita un acto posterior del sujeto pasivo. La pregunta es si podría darse esa autorización mediante un contrato de adhesión con una serie de actividades, o si se necesita la autorización

expresa de esa persona. Y en cuanto a la notificación, mi pregunta es si está contemplado también la notificación por medio de discos en un diario, en el Diario Oficial en el caso de que no se supiera el domicilio o el paradero de esa persona.

RESPUESTA DE D. FRANCISCO EUGENIO: Gracias por la pregunta. Para fijar de paso una parte de la respuesta que por mi parte omití a la primera pregunta.

Se trata en primer lugar de sentar la base de que como dice la LORTAD en el artículo 2.1.b) a los ficheros mantenidos por personas físicas con fines exclusivamente personales, no se aplican las limitaciones de la LORTAD. Los ficheros con fines puramente personales, el supuesto que yo contemplaba y no desgrané del todo, era el de un servicio de información sobre morosos, no un control sobre los propios morosos del particular.

Entonces, me parece que es oportuno decir públicamente la respuesta que da la LORTAD a ese supuesto, no es obligatoria la inscripción, la notificación.

Respecto a esta puntualización del matíz entre notificar o recibir la autorización, los textos que hemos examinado, contemplan la mayoría de ellos el principio del silencio administrativo, de manera que si no se contesta otra cosa «desde ya», que se dice en América, se puede empezar a funcionar con los ficheros, porque se entiende que el sujeto que ha presentado esa notificación asume los deberes, como dice la ley francesa, que implica la propia ley. Entonces hay la teoría del silencio administrativo tan criticada desde otros puntos de vista porque parece que denota cierta negligencia de los funcionarios, pero quizá, el propósito de la ley es agilizar la autorización, que, repito, solamente la ley española utiliza esta palabra. Los demás hablan de notificar.

Que se de por enterada la Administración, o no la Administración, este órgano público independiente que es la Agencia de Protección de Datos, o la Oficina de Control, o la Comisión General de libertades, como se llame, de forma que creo que esa es una de las preguntas que habría que atender y la otra, evidentemente hay, y no sé si he entendido bien el otro punto, un registro de ficheros, en el que se trata, efectivamente de poner a disposición del público cuáles son los ficheros autorizados, registrados, que se supone que se actualizará esta relación de ficheros inscritos en la Oficina de Control.

Y, por último, incidiendo en la primera pregunta, me permito leer de nuevo otro artículo de la LORTAD que dice que sólo podrá comprobar como si están autorizados los ficheros de morosos, que veo que el caso ha tenido tanto eco, con fines del servicio de información a las posibles víctimas futuras, se podrán registrar y ceder datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados, y que no se refieran cuando sean adversos a más de seis años. Sólo se podrá registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la

solvencia económica para los afectados, y que no se refieran, cuando sean adversos, a más de seis años. El fin de la solvencia económica no otra cosa, una utilidad jusitificada y evidentemente está patente el derecho al olvido. Esa película que es la vida que no podemos cortar y que tiene que seguir haciéndose y no vale estar siempre atados al pasado.

RESPUESTA DE D. ETIENNE MONTERO: No quiero insistir demasiado, pero quizás, creo que no se puede considerar que un fichero de abogados sea un fichero estrictamente personal. No estoy totalmente de acuerdo, por lo menos en la doctrina jurídica francesa se dice claramente que un fichero de un abogado, de un médico, de un farmacéutico, etc., son ficheros profesionales, y que hay que declarar el fichero cuando haya datos personales.

RESPUESTA DE D. FRANCISCO EUGENIO: Quizá sea una interpretación precipitada, aqui está el texto de la Norma que la jurisprudencia interpretará. Dice «con fines exclusivamente personales». Hay que ver qué sentido tiene en la ley española ese fin exclusivamente personal.

PREGUNTA: Esta mañana ha sido objeto de críticas bastante acervas el Proyecto de la Ley Española de Protección de Datos. Parece ser para el Profesor Ripol que hay un Proyecto de Directiva Comunitaria sobre esta msima materia. Entonces la ley española ¿se ajusta a esa directiva comunitaria en este punto de garantías para el particular? Si es que no se ajusta ¿no podría ser este precisamente un mecanismo de lucha contra la ley, el de acudir al Derecho Comunitario en Protección de unos Derechos que la ley española, la ley nacional, no protege lo suficiente?

RESPUESTA DE D. SANTIAGO RIPOL: En primer lugar, el Proyecto de Directiva Comunitaria es, en la actualidad, un Proyecto que se presentó en 1990, entonces, los trabajos rutinarios de aprobación normativa en la Comunidad llevan a que esto se ponga a consideración de los estados miembros, que se pongan a consideración de las diferentes empresas que intervienen en el sector, etc., y después estos formulan una serie de informes, no vinculantes, se pasa al Parlamento Europeo, que emite un nuevo informe, para después volver a la Comisión, y finalmente la aprueba el Congreso.

En Marzo del presente año, el Parlamento Europeo aprobó su informe, y en Julio, la Comisión ha elaborado una segunda propuesta o una revisión de la Propuesta de Directiva, que va a tener que ser considerada de nuevo por los Gobiernos, etc.

Quiero decir con esto que el Proyecto de Directiva es un Proyecto, y muy Proyecto todavía, que aún falta bastante en los trabajos legislativos de la Comunidad. En la actualidad, por tanto, los mecanismos de defensa con que cuenta el ciudadano español, son los establecidos en la Constitución, como derecho fundamental, recogido en el Título I, los mecanismos procesa-

les habituales, porque los mecanismos específicos que establezca la LORTAD todavía no están en vigor.

Los dos textos de la LORTAD y de la Directiva, los dos proyectos, son proyectos que no se encuentran muy disociados, es decir, los principios son los mismos, ambos remiten al texto al convenio de 1981, y a las directrices del Consejo de Europa o de la OCDE, entonces pienso que no hay una gran disociación entre el contenido de los dos textos, los derechos que se protegen son similares y, en cualquier caso, cuando se apruebe la directiva, existirá un mecanismo de protección adicional por la tutela que, efectivamente, tal y como está redactado en la actualidad, concedería derechos directos a los ciudadanos nacionales y ahí encontraríamos, por tanto, ese principio de efecto directo que puede tener el derecho comunitario, que lo único que le da al particular es el derecho a reclamar la normativa comunitaria ante un tribunal interno, ante un juez ordinario, es decir, no se podría ir al Tribunal de Justicia de Luxemburgo.

PREGUNTA: Con relación a esa regulación que se hace de la circulación de datos, en función de la Comunidad Económica Europea, esa libre circulación de datos que se busca, y en contraposición la regulación que se hace dentro de los Estados miembros, ¿se prevé que pueda haber colisiones al punto de que en el ámbito de la Comunidad Económica se puede llegar a una circulación de datos que los ámbitos locales no estén permitidos o estén sancionados de alguna forma particular?

RESPUESTA DE D. ALVARO SANCHEZ BRAVO: Evidentemente la regulación comunitaria, como apuntabamos ántes, lo que pretende es establecer una serie de medidas legislativas de base. La legislación comunitaria lo que pretende es establecer normas que, en el fondo, y sobre todo en lo referente al objeto de la protección, al sujeto de la protección a los derechos que asisten tanto a los titulares de las bases de datos como a las personas cuyos datos estén incluídos en ellos, lo que pretenden es establecer un marco global de actuación, pero fundamentándolo desde la enunciación de unos principios generales. Quizás ese es el problema que apuntabamos antes, y en el cual la situación comunitaria actual existe por un lado esa lucha entre los Estados nacionales que han legislado sobre la materia y que en algunos casos no quieren ceder parte de lo que ya han hecho al Derecho Comunitario, y el Derecho Comunitario que parece ser que va viendo cómo algunas legislaciones nacionales se van apartando de los principios básicos que deberían ser necesarios para la consecución de esa unificación legislativa.

Resumiendo, tenemos por un lado los Estados nacionales, con una legislación específica que en algunos casos no quieren someterse, al menos voluntariamente a los dictados comunitarios, y por otro lado, un Derecho Comunitario floreciente, como ha señalado el Profesor Ripol anteriormente, en la mayoría de los casos no de carácter imperativo, sino sólamente son meros

proyectos, pero que creo que tienen la eficacia de que pueden constituir la base de una futura regulación unitaria en el marco de la Comunidad, o sea, que actualmente no puede hablarse de una colisión entre la regulación comunitaria y las regulaciones nacionales, porque para el ciudadano comunitario de un Estado en el que existe regulación sobre la materia, tiene que adaptarse a las normas de los estados nacionales.

SESION III

MESA N.º 4.–CONTRATACION INFORMATICA Y PROTECCION DEL SOFTWARE

«La informática en Cuba. Algunas consideraciones acerca de la protección y comercialización del Software. Régimen de protección de los datos»

YARINA AMOROSO FERNÁNDEZ
Licenciada en Derecho. Ministerio de Justicia.
Especialista en asuntos Jurídicos
(CUBA)

A MODO DE INTRODUCCION

El Derecho estudia el fenómeno informático en su carácter de objeto, en este sentido a través de disposiciones jurídicas se establecen las normas que regulan el uso de los medios técnicos de computación, su comercialización, así como la protección de los productos informáticos y el flujo de datos transfronteras, entre otros aspectos jurídicamente tutelables.

La búsqueda de soluciones legales para dar respuestas jurídicas que se correspondan con el nivel de desarrollo actual y perspectivo de la tecnología y de las aplicaciones informáticas en Cuba, la problemática de la contratación y el régimen jurídico de protección de los datos y el software, está hoy incluída en el quehacer diario de los especialistas de esta esfera.

No es posible abarcar en tan pocas cuartillas un tema tan extenso e importante por lo que sólo expondré las etapas principales que se han desarrollado en la búsqueda de soluciones jurídicas para la protección del software y los datos en Cuba.

Un poco de historia.

Hablar de la Informática en Cuba obliga a enmarcarla en dos períodos históricos: antes y después de la Revolución.

La utilización de las técnicas de computación en Cuba se remontan al final de la década de los años veinte, con la introducción de los primeros equipos destinados al procesamiento de datos para desarrollar el Censo de Población de 1930. Después la IBM instaló en La Habana una sucursal con rango de oficina central para el Caribe y la América Central.

Desde entonces, la utilización de equipos informáticos aumentó considerablemente, de modo especial en las empresas con capital norteamericano radicadas en Cuba. Cabe recordar que en este tiempo el 90% del potencial informático se concentraba en La Habana.

Esta etapa se caracteriza por el predominio de la introducción de equipos electromecánicos de procesamiento de información en tarjetas perforadas, además del establecimiento de un monopolio que consistía no sólo en la producción y venta de los equipos que se introducían, sino también de la reparación y el mantenimiento de los mismos, así como de los servicios de diseño e implantación de los sistemas que se aplicaban, e incluso los especialistas.

Con el triunfo de la Revolución cubana en 1959, la situación cambió. El gobierno revolucionario intrudujo en el país máquinas computadoras electrónicas de la primera generación.

Luego, en 1965, adquirió computadoras de la segunda generación para el cálculo científico y la formación de especialistas informáticos.

En 1966, con las transformaciones en los programas de educación superior, se sientan las bases para la puesta en marcha en 1969 de un plan para la introducción de medios tecnológicos informáticos, pero sobre todo para empezar a desarrollar de modo independiente sus propias computadoras, con diseño y producción nacionales, así como crear un software apropiado a sus necesidades. Comienza así, una etapa en que se desarrolla un importante plan de inversiones, lo que le ha permitido en la actualidad contar con centros de adiestramiento de alto nivel, bancos de datos y fondos de programas y avanzar en el proceso planificado de informatización de sus estructuras organizativas, económicas y de dirección.

A finales del año 1969, se crean las bases para el desarrollo y producción nacional de medios de la técnica de computación, que hasta ese momento sólo se habían garantizado por la vía de las importaciones.

También en los últimos años de la década de los sesenta se dan los primeros pasos para la introducción de la especialidad como una carrera universitaria, y ya a principios del setenta se crearon diversos centros de estudios

de Informática, con el objetivo de propiciar la introducción y desarrollo de sus aplicaciones en la producción y los servicios del país.

El INSAC

Paralelamente se previó el desarrollo de instituciones en las que se confiaron las funciones de dirección y aplicación de las políticas trazadas. Así, con la promulgación de la Ley 1323 de 30 de noviembre de 1976, se creó el Instituto de Sistemas Automatizados y Técnicas de Computación (INSAC).

Esta institución de la administración central del Estado es el encargado de controlar la aplicación de la política o en las actividades relativas a los sistemas automatizados de gestión y a las técnicas informáticas, con las siguientes atribuciones y funciones:

- Elaborar y establecer principios metodológicos estandarizados y controlar su aplicación en la producción de sistemas automatizados de dirección, con el fin de asegurar que dichos principios se fundamenten en bases técnicas y económicas factibles.

- Preparar, con la asistencia de otros organismos del Estado y órganos locales del poder popular, el plan para la introducción de los sistemas automatizados de gestión y de técnicas informáticas; someterlo a la aprobación de la Junta Central de Planificación; una vez aprobado, controlar su ejecución.

- Proyectar sistemas de dirección integrados los que deben ser rentables desde el punto de vista económico. Establecer las normas para el aprovechamiento de la tecnología informática, supervisar su realización y proporcionar los servicios técnicos consecuentes.

- Organizar un red de centros informáticos de uso colectivo para que el aprovechamiento de los equipos sea más eficiente.

- Informar al Consejo de Ministros sobre la creación o disolución de los centros informáticos y de los centros de concepción de sistemas automatizados pertenecientes a la función pública.

- Promover y guiar el desarrollo de la Industria Infomática.

Este Instituto está integrado por un sistema nacional de empresas y unidades especializadas, a través de las cuales desarrolla las funciones de investigación y producción de hardware, así como los equipos auxiliares; ofrece servicios colectivos de procesamiento de datos; realiza la capacitación de personal técnico y de la asistencia especializada para la introducción de la informática, la cual comprende, entre otros: asesoría, instalación, mantenimiento, reparación de equipos y sistemas respectivamente.

La Informática: Prioridades y Futuro:

En Cuba las aplicaciones informáticas han estado dirigidas en primer término al sector productivo, cuyas áreas más priorizadas han sido el azúcar,

el hierro, la ingeniería, la construcción, el transporte y la energía. Con el desarrollo de los planes de salud, el mismo también se ha convertido en un sector priorizado en la esfera de estos servicios; además, de la actividad pública y los sistemas de educación nacional.

En la actualidad el potencial informático se encuentra distribuído a lo largo de todo el país.

En 1985, en el marco de nuevos cambios y enfoques que se empiezan a operar a nivel de nuestra economía, se constituye el Frente de la Electrónica como elemento centralizador y catalizador de los esfuerzos del país en materia de informática y electrónica. Este frente ha permitido crear un centro coordinador a nivel de gobierno para dirigir y orientar el desarrollo integral de la base productiva, investigativa y de desarrollo en materia de informática y electrónica, a partir del mismo están creadas diversas comisiones permanentes de trabajo en las que se encuentran representados todos y cada uno de los organismos implicados en la economía y los servicios.

El futuro desarrollo de las técnicas informáticas en Cuba está previsto a través de una estrategia nacional económica y social con horizonte en el año 2000. Ella contiene entre sus tareas principales:

• Desarrollar la producción en serie de equipos destinados a satisfacer la creciente demanda interna y a cumplir los compromisos contraídos con otros países.

• Desarrollar la producción de equipos y de sistemas utilizando componentes electrónicos modernos, elementos y bloques modulares sobre la base de los progresos realizados en el software básico.

• Desarrollar la producción de equipos y sistemas a partir de pequeñas series lanzadas en las unidades de investigación y de desarrollo, con el objeto de promover y potenciar el desarrollo de nuevas e importantes aplicaciones especializadas.

• Desarrollar las aplicaciones de sistemas de microcomputadoras y subsistemas de teletransmisión y teleprocesamiento de datos.

• En el campo del software, las nuevas perspectivas incluyen sistemas especiales para la gestión y el control de operaciones, para la creación de sistemas distribuídos y para la formación de redes.

Se continúa en el perfeccionamiento de nuestros planes de estudio destinados a la formación de especialistas de alta calificación, además de desarrollar la experiencia de aprendizaje masivo de las técnicas de computación en los Joven Club, organizados con el objetivo de masivizar el dominio de la técnica y preparar la generación del 2000.

También se prevé la conquista de nuevos mercados para la comercialización de nuestros productos informáticos.

A partir de 1983 irrumpen significativamente en el país las computadoras personales, y en forma ascendente comienzan a surgir alternativas nacionales para la adquisición y producción de microcomputadoras, en respuesta a la creciente demanda.

La necesidad de la Protección:

Este desarrollo impetuoso de las aplicaciones informáticas en diferentes esferas de la vida en nuestra sociedad, no tiene correspondencia en nuestro ordenamiento jurídico, ya que los instrumentos normativos con que contamos no pueden proporcionar los mecanismos legales indispensables que respalden éstos propósitos.

No obstante, el tratamiento tan amplio de algunas instituciones jurídicas permite interpretar, y de hecho han sido aplicadas, esas disposiciones a diferentes relaciones derivadas de las aplicaciones informáticas.

Por ejemplo, si analizamos a la luz de la legislación cubana vigente sobre materia de patentes – Decreto Ley No. 68 de 1983 –, la posible tutela jurídica de los programas de computación, hallamos que no existe una exclusión expresa del software como objeto patentable. Pero sí se limita su aplicación a éstos, al disponer que para recoger una invención ésta debe ser novedosa y resultado de una actividad inventiva, además de tener aplicación industrial.

Este propio Decreto-Ley regula las marcas, régimen al cual se acogen en la práctica las entidades cubanas relacionadas con la producción del software.[1]

Otra práctica que permite al menos una protección formal y que evita en lo posible usos no autorizados, es la impresión del símbolo del copyright con el nombre del titular y el año de la primera versión. Todo ello se logra en virtud de la legislación vigente en materia de Derecho de Autor –Ley No. 14 de 1974 –. Esta ley no incluye al software como objeto de protección, pero como su tutela alcanza a las obras científicas, artísticas, literarias y educacionales, que se hayan hecho o puedan hacerse de conocimiento público por cualquier medio lícito, cualesquiera que sean sus formas de expresión, su contenido, valor o destino, ello ha servido de fundamento legal para que algunos autores se acojan a esta modalidad. Se acogen a pesar de que la ley exije el requisito de originalidad, lo cual, tal como nos hemos referido con anterioridad, no es fácil de comprobar en el caso de la producción de los

[1] En la Oficina nacional de Invenciones, Información Técnica y Marca (ONITEM) se encuentran registradas ocho marcas de software nacional en la clase 9 de la clasificación Internacional de Productos y Servicios, o sea para el producto de 5 marcas en la clase 42, para la prestación de servicios. Las primeras son utilizadas por las entidades cubanas que comercializan software como productos terminados con otras empresas e instituciones nacionales y con el extranjero, mientras que las de la clase 42 son utilizadas cuando estas mismas entidades subcontratan fuerza de trabajo a otras empresas –fundamentalmente extranjeras– para realizar determinados programas y cuando elaboran software por encargo expreso de otra institución.

programas de computación; por lo que sumándonos a la práctica internacional hemos prescindido de estos análisis.

Por otra parte, este reconocimiento no contempla la inscripción en el Registro de Derecho de Autor, pues en Cuba éste se lleva exclusivamente para las obras musicales y dramático-musicales. Este vacío se suple, aunque también en el plano formal, a través del Fondo Nacional de Sistemas y Programas [2], el cual funciona como registro centralizado de los productos de programación que existen en el país.

Confidencialidad, Licencias y Certificados de Autor:

Por su parte las entidades autorizadas para la comercialización de productos informáticos se acogen a métodos tradicionales de transferencia con algunas particularidades.

Una de esas particularidades es la utilización de las cláusulas de confidencialidad o de discreción en los contratos de venta o arrendamiento, lo que encuentra respaldo legal en nuestro Código Civil. En él se establece que las partes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, salvo disposición legal en contrario. Por otra parte, se incluyen cláusulas relativas a la asistencia técnica. También se utiliza en todos los casos en que se necesita, conjuntamente con el software, el asesoramiento de personal especializado para la instalación y la adaptación del software al fin requerido, su traducción, entre otros servicios. Ante el incumplimiento de estas cláusulas se puede exigir la responsabilidad en virtud de la propia legislación civil y la penal.

Otra peculiaridad es el otorgamiento de Licencias Completas, las que se nos han impuesto dadas las limitaciones de mercado que tiene nuestro país.

Estas Licencias ceden por un período de tiempo limitado la posesión, uso, disfrute y disposición del software al licenciatario. En realidad constituye una cesión temporal de todos los derechos, apareciendo incluso el copyright a favor de la entidad extranjera receptora y su marca de comercialización.

Estas licencias otorgan a las empresas extranjeras los derechos sobre un software nacional por un período que oscila entre 2 y 3 años, mediante un royalty generalmente determinado por precio de venta. Aunque tiene un plazo límite, en realidad la mayoría de las veces constituye el máximo de explotación posible del software por la corta vida útil que éstos tienen.

Otra fórmula de protección utilizada en Cuba está amparada en la Ley No. 38 de 1982, la que establece una novedosa modalidad de protección: El Certificado de Autor de Racionalización. El mismo aplicable por interpretación a aquellos programas que ofrezcan soluciones correctas, nuevas y útiles de un problema técnico-organizativo o económico – organizativo para la enti-

[2] El Frente Nacional de la Electronica en su vigésima novena reunión efectuada en octubre de 1988 acordó la constitución del Fondo Nacional de Sistemas y Programas.

dad en la cual fue presentada y reconocido, siempre que su aplicación aporte un beneficio técnico-económico social.

Los que crean software de su contenido de trabajo, utilizan esta vía para obtener protección dentro del ámbito de su entidad y de aquellos a los que le haya enviado la información, recibiendo este Certificado y una remuneración al año de su aplicación, en correspondencia con el efecto económico o social obtenido. Los derechos de uso y explotación del software son del Estado, quien decide su aplicación y comercialización por medio de la entidad que reconoció el software como racionalización, la cual es a su vez la que aparece como titular del copyright en el programa.

Esta modalidad de protección sólo existe en Cuba. Su dificultad radica en proteger al software a nivel local o cuando más nacionalmente, pero no en el resto del mundo. Por otra parte, genera un paralelismo en los mecanismos de comercialización.

Llenar el vacío

Ante este tácito vacío jurídico el Frente Nacional para la Electrónica creó una comisión jurídica, la que viene trabajando desde hace algún tiempo para proponer la solución más adecuada en correspondencia con nuestros problemas y el nivel de desarrollo que en esta esfera tiene el país.

Para cumplir con esta tarea fue preciso elaborar un programa de trabajo que abarca cinco etapas fundamentales y en las que es necesaria la labor constante y minuciosa de los especialistas.

En la primera etapa está comprendida la revisión y estudio de la legislación y de documentos jurídicos o no; tanto de carácter nacional o internacional; haciendo especial referencia a estos últimos y que se refieren a la problemática del software.

Estas tareas de revisión y análisis tienen por objetivo evaluar los resultados nacionales en los intentos de brindar protección al sotfware, sistematizar las disposiciones que existen, así como dar respuesta jurídica a los aspectos que no han sido regulados hasta el momento. También conocer y valorar la experiencia internacional sobre la materia para atemperar, en lo posible, nuestra legislación a las soluciones jurídicas de otros países, teniendo en cuenta las relaciones de intercambio comercial de Cuba en este campo.

Sin embargo, es menester aclarar que no se trata de la suma aritmética de experiencias, ni la transpolación de normas para ser aplicadas en nuestro país, sino que se trabaja bajo el principio de proponer una legislación acorde a nuestras necesidades actuales y futuras.

La segunda etapa comprende la evaluación de la eficacia de las normativas internas vigentes.

Mientras que la tercera consiste en valorar el estado actual de desarrollo de la aplicación de la Informática en Cuba y sus perspectivas, para que acorde

con la Política Nacional Informática se pueda determinar cuáles son las aplicaciones actuales y perspectivas.

Consideramos que ambas son etapas medulares, ya que las mismas aportarán a la nueva legislación el objeto a regular y tutelar, así como los elementos fundamentales que garanticen la eficacia de su complimiento y vigencia en el tiempo y que las normas que se aprueben sean el reflejo fiel de la política en materia de protección y comercialización del software.

Las etapas cuatro y cinco son etapas culminatorias y consisten en la elaboración de las bases y el anteproyecto de disposición jurídica y el traslado del mismo al órgano legislativo competente para su análisis y aprobación.

Los resultados de estudios preliminares aconsejan articular un régimen de protección especial, independiente y complementario que incluya explícitamente al software, y que en sí mismo supere las limitaciones existentes en las formas de protección utilizadas, las que tal como se han ido exponiendo no se avienen con las características de los programas de computación cuya esencia es abstracta e intangible y aun cuando se soportan en un disquete o cinta magnética, su verdadero significado y novedad reside en el esquema mental del lenguaje utilizado.

Este régimen especial debe ofrecer un marco jurídico apropiado para la protección de los derechos de los titulares acorde con nuestras condiciones, asi como delimitar el alcance de la divulgación de nuestros productos y los mecanismos para su comercialización, los cuales deben responder a una estrategia única a nivel nacional con el objetivo de facilitar la uniformidad a los fines del desarrollo.

Es consustancial a la articulación de este régimen especial replantearse la función del Fondo Nacional de Sistemas, concebido en la actualidad sólo como entidad para ofrecer gratuitamente servicios informativos, distibución de detectores y descontaminadores de virus informáticos y catálogos, entre otras útiles ofertas, lo cual a nuestro juicio debe mantenerse, pero ampliarse su función como registro de software, en tanto se instituya como registro único destinado a su protección legal.

Régimen de Protección de los Datos:

Si por un lado la informatización es sinónimo de progresos en lo tocante a la organización y rapidez de acceso a la información en general, por otro es portadora de determinados riesgos y problemas que despiertan la preocupación de los usuarios y especialistas, entre los que sobresale el de la protección de los datos.

Cada vez con más frecuencia, es común hallar en los medios de comunicación, informaciones acerca de los perjuicios causados por los virus de computadora o de sujetos que se valen de la Informática y de sus bondades para practicar actos ilícitos y adoptar conductas ilegales, no éticas, o no autoriza-

das, para penetrar en los sistemas de información, logrando incluso destruir o alterar los datos grabados en medios computacionales.

Este problema no es exclusivo de un grupo determinado de países, aunque en algunos se manifiesta en grandes dimensiones. El riesgo de ser sujeto de tales conductas es casi consustancial al desarrollo de las aplicaciones informáticas, pues como se conoce, nuevos adelantos generan nuevos problemas, los que a su vez exigen una respuesta desde el ámbito del Derecho.

Como expresamos, la informática es una realidad en casi todos las actividades de la sociedad cubana, ya que con mayor o menor rapidez las viejas estructuras informativas y de gestión se rinden ante el progreso tecnológico y son sustituídas por novedosos sistemas de información.

Es por ello, que conjuntamente con la informatización de los principales registros, se están tomando medidas encaminadas a garantizar la protección de los datos, con el objetivo de preservar el dato electrónico contra factores tanto objetivos como subjetivos. Estos últimos generados por conductas negligentes, culposas o inexpertas, las que condicionan el riesgo de pérdidas, alteración, sustracción o uso inadecuado de la información almacenada en soportes magnéticos.

Datos en Peligro:

En sentido general las primeras medidas estuvieron encaminadas a establecer un Sistema Unico Nacional para comunicar la presencia de virus de computadoras en el país; asi como a fomentar una cultura de protección en el personal dirigente, técnico y usuario vinculados a la computación. También se crearon las condiciones para desarrollar la investigación técnica de los virus que nos han atacado y de sus orígenes, así como el establecimiento de las cadenas de contaminación. Al mismo tiempo que se han puesto en práctica un conjunto de medidas técnicas y organizativas de rápida implementación por parte de las entidades usuarias de las técnicas de computación que permitan prevenir, detectar y minimizar la acción de los virus.

Mas la lucha contra los denominados virus de computadoras es sólo una parte del problema. El virus es nocivo al dato en su unidad física y entorno inmediato, y es una realidad con la que hay que aprender a convivir. La protección de los datos es un concepto más amplio, cuyos efectos jurídicos se manifiestan principalmente en tres áreas del Derecho: la penal, civil y la del trabajo.

La destrucción, manipulación, adulteración o divulgación no autorizada de datos puede ser causada básicamente, por problemas técnicos, desastres naturales y por seres humanos; estos últimos los más comunes y que mayores preocupaciones traen para aquel que tiene informaciones o que tiene el deber de protegerlas de los peligros que semejantes eventualidades pueden producir.

Por tal razón el Grupo de Expertos de Protección de Datos comenzó además a trabajar en la adecuación de un régimen legal de protección de los datos.

En esta ocasión se planteó también como principio de trabajo la revisión y el estudio de la legislación nacional y extranjera que se refiere al tema.

Entre algunas soluciones jurídicas a encontrar está la de establecer quién y de qué forma está facultado a solicitar información; qué medios aseguran la exactitud de los datos en los sistemas informativos; qué garantía de protección a los datos se establecen y su eficacia; así como quién determina y con qué objetivos puede accederse a los mismos.

Otro de los objetivos es establecer las normas para regular la disciplina informática en los órganos y entidades de la Administración Central del Estado y sus dependencias, así como las organizaciones sociales, de masas y políticas que utilizan estas técnicas, con el objetivo de garantizar la integridad y seguridad de los datos que se procesan con medios técnicos de computación, así como su uso.

Por otra parte, la protección de los datos a nuestro modo de ver abarca además los regímenes de importación y exportación de productos informáticos, específicamente los soportes magnéticos. Por lo que las normas jurídicas de protección se hacen extensivas a las normas de control aduanero. Como se conoce, la difusión de la informática da origen también a nuevas formas delictivas, las cuales utilizan los sistemas informáticos como medio de comisión, o bien que tienen a éstos en parte o en todo como su objeto.

Si bien aún en nuestro país no se han presentado problemas de esta naturaleza, es previsible que la difusión de las aplicaciones propicie que se generen. Por ello se estudia entre las soluciones jurídicas de protección de datos, prever sanciones a conductas que atenten contra la integridad de los datos. En una primera etapa en correspondencia con las aplicaciones y la legislación vigente la solución que se propone es la represión por la vía administrativa en relación al daño que se cause.

Sin embargo existe consenso entre los especialistas en torno a una necesaria inclusión en el Código Penal de figuras delictivas que contengan estas acciones, pues la ausencia de figuras concretas que se puedan aplicar a tales conductas, conducirían a que los autores de estos hechos quedarían ante la ley en franca impunidad, o de lo contrario, obligaría al tribunal a aplicar preceptos que no se ajustan con la naturaleza de los hechos que se cometen.

Conscientes que todas estas normas deben estar respaldadas por un mecanismo que facilite comprobar y evaluar el cumplimiento de los principios que en ellas se recojan, se prevé establecer además las disposiciones relativas a los procesos de Auditoría Informática, partiendo del hecho de que a través de los mismos se puede controlar la actividad informática desde la entrega de los medios técnicos, la verificación de su utilización en correspondencia

con los programas, la obtención de beneficios, la calidad de los sistemas que se utilizan, la detección de trampas en los mismos y la correcta aplicación del diseño, incluyendo la protección de los datos.

Respuesta Integral:

De modo que se trabaja por presentar una propuesta que abarque de forma integral todos los aspectos del problema, con un alto nivel jerárquico y que se haga extensiva a cuestiones tan importantes como el método de recolección de los datos, la disposición sobre la presencia obligatoria de la información, el procedimiento de protección de los datos y el control centralizado de actividad informativa y que sistematice las normas legales referentes a algunos sistemas de información.

Se debe brindar una legislación de carácter general que comprenda los aspectos comunes al registro y procesamiento de los datos y que facilite el tratamiento especial de algunos casos, como el dato contentivo de información clasificada.

Se labora en una propuesta de disposición acorde a nuestras necesidades, pero que encierre en sí, y visto desde nuestro prisma, el espíritu del concepto de protección de datos en su acepción más moderna del cual se ha hecho referencia en múltiples obras sobre la materia y en base al estudio de los principios casi universalmente reconocidos y recogidos en varias legislaciones de diferentes países. Ellos accionarán en la legislación cubana en el contexto de nuestras relaciones económicas y sociales.

La técnica legislativa que emplearemos estará en correspondencia con el estudio que se viene realizando. La disposición jurídica que se proponga debe responder también al contexto jurídico en que viene a ingresar y del lugar que ocupará dentro del Sistema de Derecho, donde encuentra su fundamento en cuerpos jurídicos tales como: la Constitución de la República de Cuba, los Códigos Civil y Penal, La Ley de Secreto estatal y la de Registro Civil, por sólo citar algunos ejemplos. En general, estas son las consideraciones acerca de un régimen de protección de datos que comienza a desarrollarse en el país.

Sólo nos resta decir que dada la naturaleza de nuestro sistema social, la legislación responde a los intereses de la sociedad. Las normas que se propongan y aprueben referentes a la protección de los datos no serán una excepción: las garantías constitucionales sobre la inviolabilidad de la información se materializarán a través de la propuesta, como en otras normas legales vigentes.

Protección Jurídica del Software en el derecho uruguayo

MARCELO BAUZA REILLY

Doctor en Derecho y Ciencias Sociales por la Universidad de Uruguay.

Diploma de Estudios Profundizados en Informática Jurídica y Derecho de la Informática por la Universidad de Montpellier (IRETIJ).

(URUGUAY)

I. INTRODUCCION

Según la doctrina extranjera especializada (VIVANT, 1989), la protección jurídica del software se organiza a través de dos grandes sendas jurídicas: las protecciones «no privativas» y las «privativas».

La primera de esas sendas comprende la protección «penal» (que intenta hacer aplicables a la materia aquellas normas sobre violación de secretos de empresa, secreto profesional y corrupción administrativa); y la protección «civil» que se subdivide, a su vez, en «contractual» (en el marco de una relación de trabajo o fuera de ella), y «extracontractual» (responsabilidad civil, concurrencia desleal, enriquecimiento sin causa).

La «protección privativa», por su parte, comprende en el estado actual del derecho comparado, los «mecanismos sui géneris» al estilo de las proposiciones de la OMPI (reglas de 1977 y proyecto de tratado de 1983) y el recurso al «derecho de la propiedad intelectual»; esto último puede venir por la vía del «derecho de la propiedad literaria y artística» comúnmente conocida como régimen de «derechos de autor» (posición de mayor predicamento

actualmente), o por la vía del «derecho de la propiedad industrial» que también tiene sus brazos diferenciados en el «derecho de patentes», el de «diseños y modelos» y el de «marcas».

II. EL MARCO CONSTITUCIONAL Y LEGAL URUGUAYO

En materia de soportes lógicos de información, Uruguay no cuenta aún con disposiciones legislativas específicas, al estilo de las contenidas en el Título VII del Libro I (arts. 95 a 100) de la Ley española 22/1987 de Propiedad Intelectual (ley del 11 de noviembre, «BOE» núm. 275 de 17 de noviembre de 1987).

Sin embargo, ello no es óbice a que pueda considerarse que el país sigue la tendencia universal en la materia, puesto que posee normas que, aún sin ser especiales, conforman un marco de protección medianamente aceptable.

En primer lugar está la propia Constitución Uruguaya, cuyo art. 33 establece: «El trabajo intelectual, el derecho de autor, del inventor o del artista, serán reconocidos y protegidos por la ley».

También el art. 7 del máximo cuerpo normativo alude a la protección del «trabajo» aunque sin el aditamento específico de «intelectual» que practica el art. 33. («los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme las leyes que se establecieren por razones de interés general»).

Estos mandatos constitucionales de reconocimiento y protección resultan de aplicación inmediata en virtud del art. 332 del mismo cuerpo, que dice: «Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas».

Como se aprecia, el art. 33 comienza sabiamente por aludir al género «trabajo intelectual» lo cual facilita la tarea del intérprete. En efecto, el juego de las disposiciones antes enunciadas permite considerar que en caso de que no se considerara regulados a los programas de ordenador por un régimen legal específico, de todas maneras debe aplicársele alguno en vía analógica. Y en tal caso, en el panorama legislativo actual de nuestro país no se encuentra otra normativa más adaptable a estos fines que la de «derechos de autor».

Pero podemos forzar aún más las cosas y sostener que, de todas maneras, no existe consagrado expresamente en la Constitución un derecho, deber o garantía que aluda en concreto a la protección de los soportes lógicos de información. En ese caso todavía podemos acudir al art. 72 de la Carta

Magna, que expresa: «La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana se derivan de la forma republicana de gobierno.

De todas maneras, como decíamos antes no se conocen voces disonantes en la doctrina nacional en el sentido de considerar alcanzados a los soportes lógicos de información por el «derecho de autor». Y Uruguay cuenta con un régimen legal específico de propiedad autoral, que la incipiente doctrina informático-jurídica acepta y se esfuerza en adaptarlo a la materia. En ello se sigue la tendencia mayoritaria de los países donde se viene actuando en forma similar, al acotarse o descartarse otras vías de protección legal (propiedad industrial, reglas OMPI).

Al igual que en esos países, el régimen de la propiedad autoral parece ser el ancla a la que aferrarse siquiera provisoriamente, dentro de un mar embravecido donde ondean poderosos intereses y singulares confrontaciones de mercado.

Dejando a un lado, pues, las protecciones de tipo «no privativo», el objeto central de este trabajo es el de dar a conocer este régimen nacional de la propiedad autoral, con particular énfasis en aquellas cuestiones más directamente vinculadas con la aplicación de dicho régimen a los programas de ordenador y sus anexos (protección privativa).

III. LA LEY DE DERECHOS DE AUTOR NUM. 9739 DE 17-12-937

Inútil recalcar que a la época de sanción de esta ley no existían los programas de ordenador y, por lo tanto, el régimen no fue legislado originariamente a los fines de proteger este nuevo tipo de obras del intelecto. Por lo demás, el mencionado régimen no sufrió mayores modificaciones o reformas posteriores, con excepción de las que se comentarán.

Sin embargo, los conceptos que maneja el legislador de la época son de tal flexibilidad que permiten incluir actualmente, y sin hesitaciones, dichos programas dentro del ámbito de protección de estas normas.

Coadyuva a dicha posibilidad la generosa redacción del art. 5 de la ley, que haciendo una larga ennumeración de las diferentes obras protegidas remata en la expresión omnicomprensiva de «y, en fin, toda producción del dominio de la inteligencia». Siendo de tal naturaleza el programa de ordenador, no hay inconvenientes de principio para considerarlos incluídos dentro de este régimen de protección legal.

Las notas esenciales del régimen (que está reglamentado por decreto del 21-04-938), son las siguientes:

– el derecho de propiedad intelectual comprende las facultades de enajenar, reproducir, publicar, traducir, ejecutar, difundir de cualquier forma y representar o autorizar a otros a que lo hagan (art.2);

– se prevee la inscripción registral de la obra a cargo de la Biblioteca Nacional (art. 6 inc. 1 y cap. XI);

– en el caso de obras extranjeras, basta probar el cumplimiento de los requisitos de protección exigidos en el país de origen (art. 6 inc. 2);

– se establecen y regulan las calidades de los titulares de derecho, a saber: autor y sucesores, colaboradores, adquirentes a cualquier título, traductores y adaptadores, intérpretes, y el Estado (caps. II a VIII);

– se establecen y regulan los casos de reproducción de la obra, tanto lícita como ilícita (cap. IX);

– se incluye un capítulo de sanciones, que contiene las previsiones específicamente protectoras y represoras en la materia: acción penal, decomiso, acción civil y protección administrativa (cap. X);

– conservación de derechos: el autor por toda su vida (art. 14), los herederos o legatarios por cuarenta años luego del deceso de aquél (art. 14), el adquirente por quince años luego de fallecido el autor a efectos de la explotación económica solamente (art. 33).

IV. LA RATIFICACION DEL CONVENIO DE BERNA

El Decreto-ley 14.910 de 19-07-979 ratificó, entre otras normas de carácter internacional, el Convenio de Berna para la protección de obras literarias y artísticas del 09-09-886 (revisado en París el 24-07-971), y el Convenio constitutivo de la O.M.P.I.

De esta manera, Uruguay se puso a tono luego de bastante tiempo de rémora, con las exigencias internacionales en esta materia, considerándose de ahí en más como derecho vigente a la normativa aprobada, en coexistencia más o menos pacífica con la norma nacional antedicha.

V. LAS REFORMAS PARCIALES DE LA LEY DE DERECHOS DE AUTOR

El capítulo X de la ley sobre «sanciones» estatuye los accionamientos concretos para la protección autoral.

No obstante la antigüedad de la ley, y las críticas que mereciera este capítulo derivadas fundamentalmente de la levedad de sus figuras incriminantes, el mismo nunca había sido reformado hasta hace poco tiempo atrás.

El art. 23 de la ley 15.913 de 27-11-987 confirió una nueva redacción al art. 46 de la ley madre mejorándola sustancialmente, en especial por lo que tiene que ver con la pena aplicable a los ilícitos autorales, que pasan de multa o prisión equivalente en la norma original a un guarismo mínimo de prisión y uno máximo de penitenciaría en el nuevo texto vigente.

Expresa la norma en su redacción actual: «El que edite, venda o reproduzca o hiciere reproducir por cualquier medio o instrumento, total o parcialmente, una obra inédita o publicada sin autorización escrita de su autor o causahabiente o de su adquirente a cualquier título o la atribuya a autor distinto, contraviniendo en cualquier forma lo dispuesto en la presente ley, será castigado con pena de 3 meses de prisión a 3 años de penitenciaría».

El art. 328 de la Ley 16.170 de 28-12-990, por su parte, modificó el art. 47 de la Ley madre que quedó redactado de la siguiente manera:

«Los ejemplares reproducidos ilícitamente y el material empleado para la reproducción, comunicación o ejecución pública, serán decomisados.El interesado podrá solicitar, como diligencia preparatoria, el secuestro de aquéllos, quedando el Juez facultado para eximirle de contracautela cuando existan motivos fundados para ello.

La sentencia condenatoria deberá ordenar en todo caso la destrucción o inutilización de los ejemplares y material decomisado cuando ellos sean susceptibles de utilización y en la medida necesaria para impedir la explotación ilícita. No se destruirán aquellos ejemplares que hayan sido adquiridos por terceros de buena fe, para su uso personal».

VI. ALGUNAS OTRAS NORMAS DE NATURALEZA ADMINISTRATIVA

El panorama normativo que se expone no estaría completo si se dejaran a un lado algunas otras normas que, aunque de una jerarquía jurídica inferior, juegan su rol en la materia esta vez en forma específica.

El Decreto Nº 154/989 del 11-04-989, a raíz de un pronunciamiento anterior del Consejo de Derechos de Autor, modificó el art. 19 del Decreto reglamentario de la Ley 9.739, para dar cabida a la inscripción de los programas de ordenador en el registro general de obras que lleva la Biblioteca Nacional.

En su mérito, a partir de la reforma dicho art. 19 ha quedado redactado así:

«Para el registro de fotografías, planos, mapas, fonogramas y programas de ordenador, se depositarán dos copias de los mismos. Las copias de los programas de ordenador podrán depositarse enteras o trechos de las mismas suficientes para caracterizar la creación del programa. Las informaciones que fundamenten el Registro de programas de ordenador tendrán carácter secreto, no pudiendo revelarse sino para su examen, por el Consejo de Derechos de Autor, a requerimiento del propio titular o por orden judicial».

En otro orden de protecciones y regularización de situaciones anormales que se venían dando en la práctica, se dictó otro Decreto el 06-02-91 atento a «la necesidad de regular el uso legítimo de programas de computación en

la Administración Pública a fin de evitar la copia ilegítima de los mismos» (considerando del propio Decreto), que se transcribe a continuación:

«Artículo 1º.– En todos los casos en que el Estado incorpore soportes lógicos para su parque de computación y cualquiera que fuere la modalidad utilizada para ello (compra, arrendamiento, licencia de uso u otras), de forma gratuita u onerosa, deberá verificar previamente la titularidad del programa de computador;

Artículo 2º.– Cuando se trate de soporte lógico de origen nacional, se exigirá al proveedor la presentación del correspondiente certificado del Registro de Derechos de Autor que expide la Biblioteca Nacional, a fin de comprobar la titularidad del mismo;

Artículo 3º.– Cuando se trate de soportes lógicos que no sean nacionales, el proveedor deberá acreditar fehacientemente la titularidad de los derechos que negocia con el Estado».

VII. CONCLUSION

A través de las transcripciones y comentarios efectuados, surge que Uruguay cuenta con un régimen jurídico protector para los programas de ordenador (o soportes lógicos de información), de tipo privativo.

Si bien dicho régimen no prevee, hasta el presente, disposiciones específicas que atiendan la problemática particular de este tipo de bienes inmateriales, el mismo queda encartado sin demasiadas dificultades de interpretación bajo dos planos jurídicos conectados y hasta preordenados jerárquicamente uno del otro:

– El sistema de derechos, deberes y garantías constitucionales, particularmente por lo que dice relación con la protección del «trabajo intelectual», la aplicación inmediata y la extensión analógica de dicho sistema protector, sin necesidad de ley específica que la reglamente (arts. 7, 33, 72, 332 de la Carta Magna).

– La Ley nacional de propiedad artística y literaria que, si bien es de cierta antigüedad, contiene el único régimen actualmente asimilable para organizar una protección de tipo privativo, posición que asume la doctrina nacional apelando al sentido amplio y abierto de la ley, y siguiendo en ello cierta corriente predominante del Derecho comparado; régimen que, por lo demás, ha sido actualizado parcialmente en alguna de sus normas, pretendiendo dotarlo de garantías más efectivas que las que consagraba el texto original.

– Por debajo de los niveles de la Constitución y la ley encontramos sí algunas pocas normas específicas, de naturaleza administrativa, dirigidas a atender alguno que otro aspecto particular o sectorial del marco protector.

Es deseable que en un futuro cercano se dicten normas legales que se ocupen específicamente de la protección de estos bienes. El Parlamento nacional tiene a estudio una reforma completa del régimen de la propiedad autoral que contempla esta necesidad, de cuya fecha de aprobación no existen signos ostensibles hasta el presente. De todas maneras, la difusión acelerada que viene experimentando el uso de la informática en el país, y la necesidad de proteger más específica y más eficazmente a quienes crean programas de ordenador, sean nacionales como extranjeros, hace suponer que el cambio no habrá de demorar demasiado

BIBLIOGRAFIA

BARRETO GUGELMEIER, Mario, «Proteccion jurídica del software, bases de datos y circuitos integrados», Buenos Aires, folleto editado por el PNUD dentro del Programa Regional de Cooperación en Informática y Microelectrónica (RLA/86/003), 1991, 65 pp.

BOLETIN OFICIAL DEL ESTADO, «Código de legislación informática», Madrid, *ed. BOE*, 1988, 653 pp. (p. 338).

DELPIAZZO, C., «Información, Informática y Derecho», Montevideo, *ed. Amalio M. Fernández*, 1989, 124 pp.

VARIOS AUTORES, «Propiedad incorporal, derechos de autor y conexos, propiedad industrial y marcaria, trabajos de las Primeras Jornadas Uruguayo-Argentino-Brasileñas sobre Propiedad Incorporal (1985)», Montevideo, *ed. Min. Educ. Cultura*, 1987, 207 pp.

VIVANT, M. y otros, «Lamy droit de l'informatique», París, *ed. Lamy*, 1989, pp. 621-751.

Contrato de arrendamiento sobre bienes informáticos

JUAN C. BENITO-BUTRÓN OCHOA

Letrado Administración Seguridad Social. Abogado Economista. Titulado Superior de Relaciones Ind.

(ESPAÑA)

SUMARIO

I. INTRODUCCION A LA CONTRATACION INFORMATICA

II. BIEN INFORMATICO (COSA EN SENTIDO JURIDICO) Y CONTRATO DE ARRENDAMIENTO

III. ESPECIALES ARRENDAMIENTOS SOBRE BIENES INFORMATICOS: BACK UP CONTRACT Y TURN-KEY PACKAGE

IV. OBLIGACIONES ESPECIALES DEL ARRENDADOR

V. CONCLUSIONES

VI. BIBLIOGRAFIA

I. INTRODUCCION A LA CONTRATACION INFORMATICA

La equivocidad del término «contratación informática» obliga a un previo deslinde de los significantes que pretendemos abordar. No es objeto de la presente exposición, la ejecución, realización o cumplimiento de los contratos a través de medios informatizados (contratación electrónica).

Muy al contrario, se desea acometer específicamente el estudio de un contrato (arrendamiento sobre bienes informáticos), cuyo objeto viene constituido por un bien informático, es decir, hablamos de contratos con prestación informática.

Ya adelantamos que la tipología contractual (compra venta, arrendamiento, leasing ...) no presenta grandes diferencias respecto de la general conocida al uso en el Derecho común. No obstante, si bien es cierto que, creemos, no se requiere una especial rama del Derecho para su estudio (obligaciones y contratos informáticos), no lo es menos que las cuestiones y problemáticas concretas, que de hecho se arrojan al devenir práctico y cotidiano están necesitados de una especifidad jurídica que debe afectar su conocimiento.

II. BIEN INFORMATICO (COSA EN SENTIDO JURIDICO) Y CONTRATO DE ARRENDAMIENTO.

El objeto del contrato informático, esa entidad o bien sometido al poder o señorío de la voluntad del titular o sujeto del derecho subjetivo que le sirva de medio para sus fines, no puede ser otro que el bien informático (al margen del servicio que no tratamos), la cosa objeto de la relación jurídica contractual, el ordenador como sistema de tratamiento automatizado de la información.

El ordenador o «computer» que constituye el bien, cosa u objeto contractual, está compuesto físicamente por diversas unidades o elementos: la parte material o mecánica (hardware) con instrucciones u órdenes lógicas llamadas programas, y la parte intelectual (software) o soporte lógico de tales instrucciones y órdenes.

Luego, el contrato de arrendamiento sobre bienes de equipamiento informático, comprende aquél cuyo objeto básico consiste en la traslación o cesión temporal del uso y disfrute del ordenador considerado en su conjunto (hardware y software, más aplicaciones y programas) o en alguno de sus componentes de manera individual o separada, a cambio de un precio cierto.

Por lo tanto aludimos a un contrato consensual bilateral, oneroso (a diferencia del comodato), conmutativo, traslativo del uso y disfrute (a diferencia de la compraventa) y temporal (a diferencia del usufructo) al que podemos apellidar como Arrendamiento de Casa (Locatio rerum de Art. 1543 CC), mueble (alquiler) compuesta (hardware y/o software y/o programas de aplicación).

Distinto del nuestro es el Arrendamiento Financiero o Leasing, (que propiamente queda limitado o circunscrito al hardware, puesto que el software difícilmente puede ser objeto de opción compra), cuyas particularidades no podemos señalar por mor de la brevedad.

Es de destacar la importancia de la designación, identificación, delimitación o determinación del material informático objeto del contrato, pues deviene esencialmente relevante una clarificación plausible del contenido y efectos posteriores en la vida del contrato.

La Directiva 91/250/CEE sobre protección jurídica de los programas de ordenador, menciona en sus consideraciones previas el «Alquiler» de programas de ordenador o copias.

III. ESPECIALES ARRENDAMIENTOS SOBRE BIENES INFORMATICOS: BACK UP CONTRACT Y TURN-KEY PACKAGE.

Dentro del genuino Arrendamiento de cosa o bien informático podemos incluir el «BACK UP CONTRACT» como negocio jurídico patrimonial del carácter bilateral cuya finalidad es asegurar el mantenimiento de la actividad (empresarial) para el supuesto de que circunstancias previstas pero inevitables impidan, de forma continuada utilizar los propios instrumentos informáticos, poniendo a disposición del arrendatario los elementos informáticos pactados, con el arrendador.

Viene a ser una especie de medida de aseguramiento mediante recambio temporal o sustitución pactada que empieza a florecer en los mercados de la contratación informática al abur del avance tecnológico y la expansión empresarial.

Nuevamente adquiere vital importancia el clausulado contractual donde han de quedar perfectamente delimitadas las circunstancias o motivos que causan esa imposibilidad manifiesta y temporal (no momentánea o provisional como pueden ser las coloquialmente llamadas «caídas de línea»), normalmente no imputable al arrendatario, cuya interpretación se convierte en la mayoría de los casos en caballo de batalla judicial. De igual forma el tiempo; modo o manera de utilización; las garantías de preaviso y mantenimiento; así como la premisa ineludible de la compatibilidad de sistemas informáticos, requieren una lectura o compromiso detallado a la hora de celebrar este contrato. Especial relieve debe darse a las reglas de responsabilidad derivada para el supuesto de daños ocasionados con motivo del uso o disfrute del ordenador o sus componentes.

Distinto del anterior, por situarse más bién a horcajadas entre el arrendamiento de servicios informáticos y el arrendamiento de obra informática es el «TURN-KEY PACKAGE» o «contrato de llaves en mano» en el cual la contraprestación que se compromete puede ser una obligación de medios o una obligación de resultado. Consiste en encargar a técnico especializado la creación de un bien informático (normalmente programas de ordenador) conforme a las pautas, criterios o necesidades perfiladas de antemano, incluyendo el suministro de material informático hasta la puesta en marcha o arranque satisfactorio del mismo.

Su naturaleza jurídica es muy discutida y por lo mismo, la regulación jurídica que rija su contenido obligacional se halla enmarañada en continuos escarceos doctrinales. Así podemos citar entre otras, la problemática de la específica extinción por desistimiento unilateral del comitente y posible indemnización de daños y perjuicios.

IV. OBLIGACIONES ESPECIFICAS DEL ARRENDADOR

Además de las genéricas recogidas en el Art. 1554 CC; entrega de la cosa en tiempo y lugar determinados, con accesorios y en buen estado; reparaciones necesarias para la conservación; y mantenimiento en el goce pacífico, existen otras obligaciones específicas, y a veces accesorias, que deben merecer especial atención.

Nos referimos a los deberes de información y colaboración contínua, como verdadera asistencia técnica permanente de tracto sucesivo que acompaña el cumplimiento íntegro de la mayoría de los contratos informáticos y que suelen ir precedidos de una instrucción o formación inicial en el manejo del equipo con entrega de instrucciones o documentación pertinente al uso. Se trata de una obligación de consejo o información que ha de entenderse ínsita aún su falta de acuerdo expreso, como bien viene demostrando la práctica mercantil, quizás en aras de un mal llamado marketing o «clientelismo».

Del mismo modo podemos matizar que la obligación de reparar lo necesario para el buen uso o estado del equipo informático, lleva inserta idéntica extensión en el mantenimiento, sin que se nos oculte la dificultad de delimitación de su extensión o cobertura: uso ordinario o especial, caso fortuito, fuerza mayor, desgaste, reconstrucción...

Respecto a las obligaciones de garantía y responsabilidad, destacar tres aspectos: la palmaria garantía sobre hechos propios del arrendador que conlleva el no permitir la ulterior variación en la forma y contenido de los programas y compatibilidad informática; sobre hechos ajenos o de tercero, dependiendo de la autorización realizada en el contrato principal (es habitual encontrarse con la cláusula de estilo de exoneración de responsabilidad por los daños producidos por terceros no autorizados); y por fin la responsabilidad por vicios ocultos del bien objeto de la prestación informática y el saneamiento por evicción que se prestan a un detenido estudio imposible en estos momentos.

V. CONCLUSIONES

Las relaciones comerciales en auge y el cambio incesante de las tecnologías informáticas denotan un nuevo escenario jurídico-informático al que deben adaptarse los ordenamientos y regulaciones en general.

No obstante, es cierto que la tipología contractual informática al uso no difiere de la normal o común regulada por nuestro Derecho Civil, pero no es menos cierto que las especificidades que de hecho existen, (no sólo en atención al objeto contractual sino incluso a la formación, eficacia y prestaciones accesorias que puedan pactarse) requieren siquiera de una de las matizaciones jurídicas que deberán realizarse en un futuro no muy lejano.

Los caracteres específicos de los bienes y servicios informáticos en el contrato de arrendamiento (como en cualquiera de los tipos contractuales) hacen que las interpretaciones principales y reglas pensadas en un primer momento, para casos o bienes más tangibles (el inmueble es el bien por antonomasia de nuestro Código Civil), no se acomoden o adapten a la realidad del tráfico informático actual. De ahí que sin estrechez de miras, se postula desde ámbitos doctrinales muy variados la necesidad de una regulación específica que impida las constantes aberraciones a que puedan conducirnos nuestras máximas jurídicas generales si son aplicadas a rajatabla a los nuevos modelos contractuales creados por la técnica informática.

Una vez más la realidad práctica cotidiana avanza por delante del Derecho, que debe amoldarse al capricho de su dictado.

VI. BIBLIOGRAFIA

DÁVARA RODRÍGUEZ, M.A. «La Contratación por medios informáticos». Encuentros sobre Informática y Derecho 1990-1991. Madrid. Universidad Pontificia de Comillas. Pag. 53 y ss.

DÍEZ PICAZO, L. y GULLÓN, A. «Sistema de Derecho Civil». Vol. III, Sexta Edición TECNOS. 1991. Madrid.

EUGENIO DÍAZ, F. «Naturaleza Jurídica de la Información». Encuentros sobre Informática y Derecho 1990-1991. Madrid. Universidad Pontificia de Comillas. Pag. 35 y ss.

GETE-ALONSO Y CALERA, M.A. «La Contratación en materia informática». Revista La Ley 19-5-1992. Madrid.

PÉREZ LUÑO, A. E. «Nuevas Tecnologías, Sociedad y Derecho». Fundesco. Madrid 1987.

REVISTA ACTUALIDAD INFORMÁTICA ARANZADI. Num. 1 al 4. «Introducción a la Informática» 1991-1992.

TÉLLEZ VALDÉS, J. «Contratos, riesgos y seguros informáticos». Universidad Nacional Autónoma de Mexico. 1988.

TORTRAS, C. «Los contratos informáticos». II Encuentro sobre Informática en las Facultades de Derecho. Madrid. Universidad Pontificia de Comillas, 1988.

Responsabilidad civil derivada de la Informática

SALVADOR DARÍO BERGEL

Doctor en Ciencias Jurídicas y Sociales. Prof. Titular de Derecho Mercantil y Derecho Económico de la Univ. Nac. de Buenos Aires. Presidente de la Asoc. Argentina de Derecho Económico. Director del Instituto de Derecho Industrial del Colegio Público de Abogados de Buenos Aires.

(ARGENTINA)

1) INTRODUCCION

El tratamiento particular de los daños generados por la actividad informática se explica en cuanto los problemas que genera tienen matices diferenciales que apuntan a la complejidad propia de la materia, a los particulares vínculos que se establecen entre las partes, al diverso grado de formación técnica de los sujetos que contratan, a la diversa posición económica de los mismos que frecuentemente se traduce en abuso de posición dominante, a la relevancia que adquiere el período pre-contractual, a las particularidades de la conformidad por entrega, con incidencia en materia de vicios redhibitorios, a los riesgos que implica el manejo de banco de datos, etc.

2) LA INFORMATICA COMO ACTIVIDAD RIESGOSA Y LA RESPONSABILIDAD OBJETIVA DERIVADA DE SU GESTION

En todo quehacer humano se puede hallar un grado más o menos elevado de peligrosidad, sea para quien lo efectúa, sea para terceros ajenos.

Las normas que sancionan la responsabilidad por actividad riesgosa no contemplan la peligrosidad como elemento raramente accidental, sino a conductas características de la actividad desarrollada.

En este sentido, la doctrina prevalente en Italia distingue entre «peligrosidad de la conducta» y «peligrosidad de la actividad considerada en sí misma». Mientras la peligrosidad de la conducta se incluye en una categoría, en la cual domina la culpa, la actividad peligrosa se inserta en otra categoría en la cual el núcleo está determinado por el elemento objetivo de la actividad misma, que es peligrosa en sí o por la naturaleza de los medios que adopta. (1)

El concepto de actividad peligrosa es por su naturaleza un concepto relativo y depende del estado de avance de la ciencia y de la técnica en un sector determinado lo que lleva a calificar de peligrosa a actividades que antes no lo eran, o, viceversa.

En este contexto ¿podemos calificar a la informática como actividad peligrosa?.

La multiplicidad de campos a los cuales se aplica, la necesaria automaticidad de los procesos en que interviene, la natural aptitud de generar daños de toda índole (contractuales, extracontractuales, a bienes, a personas, etc.) convierte a esa actividad en potencialmente peligrosa. El tema no ha dejado de preocupar a la doctrina italiana que encuentra en el art. 2050 del C. Civil una base muy importante para el tratamiento de la responsabilidad civil derivada de actividades peligrosas.

Busnelli, refiriéndose a la actividad vinculada con el software, hace referencia a la citada norma. Es verdad –señala– que la jurisprudencia es bastante cauta en la aplicación de dicha norma, aún cuando ya es principio pacífico que actividades peligrosas no son sólo aquellas previstas como tales en el texto ordenado de leyes de seguridad pública o en otras leyes especiales. Existen actividades que si bien no presentan como característica típica el requisito de peligrosidad, pueden volverse peligrosas si se las desarrolla de cierto modo, mientras que no lo son cuando se las ejerce en forma o modo distinto. Y éste, remarca el autor, podría ser precisamente el caso de las actividades conectadas con la realización de un programa, las cuales en abstracto no son peligrosas pero podrían convertirse en tales en concreto con relación a la específica operación a las que se las refiera. (2)

Alpa pareciera no comulgar con tales ideas, indicando que parece difícil considerar como peligrosa a la computadora; en todo caso, puede ser peligrosa la actividad que valiéndose de la computadora tiene, no obstante, efecto

---

(1) FRANZONI, M. «Colpa presunta e responsabilitá del debitore», Cedan, Padova 1988, pág. 90.

(2) BUSNELLI, F.D. «Introducción en Computers e responsabilitá civile», a cura di G. Alpa, Giuffre, 1986.

de creación de riesgo y que tendría la misma intensidad y medida aún si fuere confiada a la acción mecánica. [3]

Con relación específica a la responsabilidad civil derivada de la gestión de bancos de datos, Ferri, Giaccobbe y Taddei, se inclinan por considerarla actividad peligrosa, sujeta a la normativa del artículo 2050 del C. Civil. [4]

Tal vez una consideración genérica de la actividad informática peque del vicio generado por su propia amplitud; dado que en dicha actividad puede provocar daños a terceros –recordemos que nos hallamos en el campo de la responsabilidad extracontractual– por fallas atribuídas al hardware, al software, a la gestión de bancos de datos, etc.

Las situaciones que pueden presentarse son de distinta magnitud, y ello, naturalmente, puede llevar a soluciones distintas.

En materia de bancos de datos pareciera que no existen disidencias en doctrina sobre la ubicación de tal actividad en la órbita de las actividades peligrosas.

En cambio podrían plantearse en lo tocante al hardware y al software.

La producción de software para el desarrollo de actividades que pueden generar peligros (v.g. tráfico aéreo, vial, instalaciones eléctricas o nucleares, procesos industriales, etc.) debe ser considerada actividad peligrosa. Si bien es cierto que al software se lo destina a una actividad peligrosa per-se –tal como lo observa Alpa– no es menos cierto que el medio empleado genera un riesgo adicional.

Como conclusión, entendemos que corresponderá al intérprete, en cada caso, conforme a las particularidades que ofrezca, considerar o no la inclusión de la actividad informática en la categoría de actividades peligrosas a los fines del manejo del régimen probatorio.

3) RESPONSABILIDAD DEL PROVEEDOR DE EQUIPOS O SISTEMAS INFORMATICOS

En esta materia debemos diferenciar la responsabilidad contractual que contrae el fabricante-proveedor ante el usuario, de la responsabilidad que contrae ante terceros por daños causados por defectos o vicios del sistema; (de carácter extracontractual).

Nos detendremos al análisis de la primera en la cual caben señalarse dos temas básicos: el deber de obligación y consejo, a cargo del proveedor y la garantía por vicios ocultos.

---

[3] ALPA, G.: «Responsabilitá extracontrattuale ed elaboratori elettronici», en I contratti di informatica, a cura di G. Alpa y Z. Zencovich, Giuffre, 1987, pág. 87.

[4] FERRI, E., GIACCOBBE, G. y TADDEI, E. «Informática e ordinamento giuridico», Giuffre, 1988, pág. 165.

El deber de información y consejo tiene una doble faz. Por una parte importa un deber de signo positivo: informar y aconsejar conforme a las pautas imperantes en la materia; pero paralelamente importa el deber de no ser reticente, de no guardar silencio sobre situaciones, detalles y aspectos que de ser conocidos por el adquirente no habrían determinado la contratación o ella se hubiera celebrado en condiciones distintas.

El proveedor debe brindar al utilizador todos los informes necesarios acerca del equipamiento contratado. En particular debe comunicar:

a) la calidad a los bienes a que se refiere el contrato;
b) los usos posibles del material;
c) El rendimiento del equipo en el tiempo;
d) la característica de la instalación;
e) los elementos que permitan al usuario efectuar los cálculos sobre la rentabilidad del sistema adquirido, costo de adquisición, costo de mantenimiento, etc.
f) los eventuales riesgos de su utilización;
g) El impacto del sistema adquirido en la estructura de la empresa;
h) las necesidades complementarias de personal.

Las obligaciones que se ponen a cargo del proveedor parten de considerar a éste como un experto, frente a un usuario que –de común– carece de formación en la materia.

El proveedor del equipo no cumple con las obligaciones contractuales que le competen con la sola entrega del material. En materia informática es decisivo el aspecto funcional, aspecto que de ninguna forma se puede considerar cumplido con la puesta a disposición del adquirente de los elementos que componen el sistema.

Los denominados tests de aceptación que se deben cumplir una vez puesto el equipo en la sede del adquirente son indispensables para tener por perfeccionada la entrega. Aquí nace la obligación de garantía del proveedor.

Fuera de las garantías convencionales que pudieran ser estipuladas, existe una garantía legal de responder por los vicios redhibitorios, ya que compete al proveedor transmitir una posesión útil conforme a la finalidad requerida.

En nuestra materia, aún sin existir un defecto intrínseco, la cosa transmitida puede resultar impropia para su destino. Así, se ha señalado, que en materia informática la insuficiencia de la capacidad de memoria o la dilación del tiempo de respuesta, pueden impedir, sin afectar la sustancia del equipo, su normal utilización.

Se impone en consecuencia, una interpretación funcional del vicio oculto. El material tiene su importancia, mas la garantía no puede satisfacerse con ese solo recaudo. La causa del contrato para el adquirente es la informati-

zación de sus actividades para llegar a determinados fines que tuvo en mira, en forma implícita o explícita, al contratar.

4) RESPONSABILIDAD DEL PROVEEDOR DE SOFTWARE

El modo y la fase en la cual el error puede ser introducido en el programa –lo recuerda Rosello– son múltiples y en cada una de las hipótesis la inexactitud, aún mínima, puede ocasionar la quiebra de todo el sistema. [5]

En este sentido, cabe señalar que el error puede aparecer en la elaboración del algoritmo, que por constituir la base esencial del programa lo traslada a toda su secuencia, puede surgir de la traducción del programa fuente en lenguaje de máquina, o finalmente puede aparecer en la introducción del programa objeto a la máquina, para su concreta operación.

Desde otro punto de vista, el programa puede ser correcto en su concepción, más elaborado en forma negligente (v.g. carencia de un adecuado control, o de duplicación de operaciones críticas), puede ser reabastecido por el usuario con datos de entrada inexactos con inevitable error en la salida. [6]

En atención a estas circunstancias, Alpa destaca que la dificultad de caracterizar el daño derivado del software no sólo se debe al hecho de que la producción del daño es de difícil apreciación fáctica, casi imperceptible, sino también al hecho de que depende de razones de sistemática conceptual, en cuanto que doctrina y jurisprudencia, no han definido aún de modo claro y uniforme la naturaleza jurídica del software.

Esta problemática, de por sí compleja, crea dificultades tanto en la atribución de responsabilidad como en cuanto a la prueba del hecho generador del daño. Hay que tomar en consideración que en el estadio actual de la técnica resulta difícil concebir un software sin errores.

Partiendo de esta realidad, se ha propuesto en la doctrina alemana la formación de standards cuantitativos mínimos en virtud de los cuales sea posible evaluar la relevancia jurídica y por lo tanto la responsabilidad del productor por las diferencias presentadas por cierto tipo de programa.

A los fines de establecer la responsabilidad del productor, un concepto fundamental es el relativo a la definición de vicio del programa. Se lo puede conceptualizar como la disfunción entre los datos que el programa está en condiciones de elaborar y los datos que son considerados válidos en el proyecto inicial. Se trata de un vicio funcional.

En principio el software elaborado a medida debe satisfacer los requisitos contractualmente estipulados. En estos límites, el fabricante contrae una

---

[5] ROSELLO, C. «La responsabilitá da inadegunto funzionamento di programma per elaboratore ellettronico: aspetti e problemi dell ésperienza nordamericana» en Computers e responsabilitá civile, a cura di G. Alpa, Giuffré, 1985, pág. 97.

[6] ROSELLO, op. cit. pág. 98.

obligación de resultados, traducido en asegurar la aptitud del software a los requerimientos descriptos por el cliente.

En lo tocante a la responsabilidad extracontractual, cabe señalar que éste es un tema de gran relevancia económica y jurídica. La utilización masiva de la informática en diversas actividades impulsó a la doctrina norteamericana a la elaboración de hipótesis de daño causados por la disfunción de programas aplicados a estaciones aéreas, a centrales nucleares, al tráfico ferroviario, etc.

Busnelli delimita en este campo de responsabilidad, dos sectores. El primero de ellos referido al error del programa que puede provocar daños económicos a terceros determinados o determinables.

En este contexto, pareciera necesario recurrir a la norma del artículo 2043 del C. Civil italiano, dejando a salvo lo previsto por el artículo 2236, que en materia de profesiones liberales establece una limitación de responsabilidad en el supuesto que la prestación implique la solución de problemas técnicos de especial dificultad, en cuyo caso el imputado no responde sino en los supuesto de dolo o culpa grave.

El otro sector se refiere al error que puede provocar daños a la salud o a la personalidad de una pluralidad indeterminada de sujetos. Aquí, el tema es de mayor incidencia, ya que los daños ocasionados pueden llegar a ser de consideración. Para este supuesto Busnelli preconiza la aplicación de la responsabilidad consagrada por el artículo 2050 (ejercicio de actividades peligrosas). [7]

5) RESPONSABILIDAD DERIVADA DE LA GESTION DE BANCOS DE DATOS

La compilación sistemática de información mediante la aplicación de tecnologías informáticas ha producido en pocos años una verdadera revolución en muchas áreas de la actividad humana.

Paralelamente ha surgido una alerta sobre la gran aptitud evidenciada para provocar daños de muy diversa caracterización que van desde los derechos personalísimos a los derechos patrimoniales. Esto señala el creciente interés de estudiar esta temática en el ámbito de la responsabilidad civil, no sólo reparadora sino preventiva.

En el ámbito de la responsabilidad contractual cabe señalar que quien opera una base de datos y ofrece sus servicios a terceros contrae obligaciones cuyo incumplimiento puede generar un daño resarcible.

En este orden de ideas se compromete básicamente a suministrar información correcta, lo cual implica un compromiso de permanente actualización, y paralelamente, suministrarla en tiempo útil y en forma continuada de ma-

[7] BUSNELLI, F. D. op. cit. pág. 6.

nera tal que la información se halle en poder del usuario cuando éste tenga necesidad de utilizarla.

Se trata en nuestro concepto de un supuesto de responsabilidad contractual objetiva, ya que el gestor del banco de datos asume una obligación de seguridad en cuanto al contenido, exactitud y periodicidad de la información que suministre.

Esta obligación de seguridad es una obligación de resultados, y por ende, quien presta el servicio, sólo se eximirá de responsabilidad en cuanto pruebe la culpa de un tercero por quien no debe responder o bien el caso fortuito extraño a riesgo propio del sistema computarizado. [8]

Independientemente de ello, el gestor del banco de datos puede incurrir en responsabilidad por difusión de información confidencialmente suministrada por el cliente o usuario.

En tal caso, la responsabilidad se fundamenta en la violación del deber de confidencialidad (deber de seguridad, de carácter objetivo, según lo considera Bustamente Alsina), quien señala que pertenecen a este supuesto los contratos entre prestatarios de servicios de medicina prepaga, mutuales y obras sociales de asistencia de salud, así como los celebrados por titulares de tarjetas de créditos, por las empresas prestadoras, y los clientes con los bancos y entidades financieras. [9]

En lo tocante a la responsabilidad extracontractual, el tema ofrece matices del mayor interés. La posibilidad de que por su manejo distorsionado puedan ser conculcados derechos esenciales del hombre y se pueda afectar su privacidad, ha provocado una alerta generalizada que se traduce en la sanción de normas específicas y en la interpretación amplia de normas ya existentes, en función de esta nueva realidad.

Aquí, más que en cualquier otro aspecto de la responsabilidad por daños, la función preventiva cobra un papel protagónico fundamental. [10]

Es que el avance de la tecnología informática ha hecho posible compilar información en cantidades antes no imaginables, procesarla en forma mucho más completa y sistemática y difundirla en contados segundos a un ámbito infinito.

Estamos ante un supuesto en que la actividad (compilación de la información) no es peligrosa por su naturaleza, sino por la forma de su realización (utilización de la tecnología informática). La natural propensión a producir daños propios de la actividad en cuestión –se ha señalado– es tal que nos hace pensar en su calificación en términos de peligrosidad.

---

[8] VÁZQUEZ FERREIRA, R.: ponencia presentada al IV Congreso Internacional sul tema «Informática e Regolamentaziones Giuridiche», Roma mayo 1988.

[9] BUSTAMANTE ALSINA, J.: «La informática y la responsabilidad civil» en La Ley, 1987 – B, pág. 892.

[10] FERRI, E., GIACCOBBE, G. y TADDEI, E., op. cit. pág. 165 y siguientes.

6) RESPONSABILIDAD DEL CONSULTOR INFORMATICO

La complejidad de la materia informática determina que la provisión de equipos o en la instalación de sistemas se recurra al servicio de expertos o sociedades consultoras a los cuales se le asignan diversas funciones según se estipule contractualmente.

El iter que concluye con la instalación y puesta en servicio de un sistema informático tiene diversas instancias que van desde su concepción (en la faz precontractual), el estudio de las necesidades y las formas de satisfacerlas, la redacción del pliego de condiciones para su elaboración, hasta su recepción final una vez concluídos los tests de aceptación. En este largo proceso se pueden contratar los servicios de una consultora para que asista y asesore en todas las etapas o se puede limitar su intervención a alguna o algunas de ellas.

¿Cuál es el carácter de las obligaciones que asume el consultor? ¿Se trata de una obligación de medios o de resultados? No es posible formular un juicio de valor universal, dependiendo ello de las estipulaciones contractuales.

Si en función de tales estipulaciones el consejero asume la planificación total para llegar a las metas propuestas por el utilizador, su obligación será de resultados. En caso contrario, nos hallaremos ante una obligación de medios y, en consecuencia, el usuario que pretenda atribuir responsabilidad al consultor deberá aportar la prueba de la falta de consejo y su relación causal con el daño provocado.

En esta materia los Tribunales franceses han adoptado una posición pragmática, según las diversas cláusulas contractuales. Para determinar la responsabilidad del consultor, será preciso que previamente se determinen los deberes que se ponen a su cargo; algunos de ellos surgirán explícitamente del contrato y otros en forma implícita, de la naturaleza propia de la materia.

En principio, el consultor no puede limitarse a ser interlocutor del usuario y escuchar sus necesidades, sino que debe interiorizarse de todas las circunstancias relativas a la operación que va a asesorar. Este ha sido el criterio de la jurisprudencia francesa, que entra en lo que se conoce como «diligencia debida».

Tal como se ha señalado, el consultor asume la plena responsabilidad de la traducción técnica de las necesidades del usuario, de su análisis funcional, y de la elaboración del pliego de condiciones según las reglas del arte, salvo que ello se excluya expresamente del contrato. [11]

El usuario debe colaborar con el Consultor para asegurar la exacta definición de sus necesidades, así como en lo relativo a la evolución de las futuras

---

[11] POULLET, Y.: «Le droit des contrats informatiques», Precis de la Faculté de Droit de Namur, Namur, 1983, p. 134.

necesidades de la empresa a informatizar y en el análisis de oportunidad. Por su parte, el Consultor debe suministrar las técnicas de base indispensables para la apreciación de la rentabilidad del sistema; tomando igualmente a su cargo la obligación de informar al cliente las particularidades de los métodos o sistemas informáticos elegidos y los inconvenientes, aún cuando fueren menores, relacionados con las características de los materiales o técnicas utilizados. [12]

La responsabilidad del Consultor puede originarse en carencia de consejo o en la formulación de un consejo erróneo, el cual será apreciado conforme al criterio arriba mencionado de la «diligencia debida».

Según lo entiende Savatier, este criterio es de una flexibilidad pragmática. Es el Juez quien apreciará las circunstancias relativas a la urgencia, remuneración, autoridad moral del Consultor, etc.

De manera más general, se puede afirmar que corresponde al Consultor la obligación de prevenir al cliente respecto de las consecuencias dañosas que puedan sobrevenir a la elección del sistema y la de aconsejar el rechazo de la automatización si es contraproducente en atención a la organización del cliente. [13]

Corresponde igualmente al Consultor el hacer un análisis pormenorizado de las necesidades a cubrir y de los elementos a adquirir por parte del cliente, para hacer una correcta aplicación de sus conocimientos técnicos y científicos.

---

[12] POULLET, op. cit. p. 136.

[13] Sentencia de la Corte de París en la causa «Prevost vs. Scofi», «Expertises», 1980, N.º 20 y siguientes.

La protección legal del «Software» en Costa Rica

JUAN DIEGO CASTRO FERNÁNDEZ

Postgraduado en Ciencias Penales. Profesor y coordinador de la Cátedra de Derecho Penal y Procesal Penal de la Escuela Libre de Derecho de la Univ. Autónoma de Centroamérica. Director del Instituto Costarricense de Lógica, Informática y Derecho. Presidente de Juriscomputación.

PATRICIA CASTRO CARVAJAL

Abogada penalista. Notario Público.

(COSTA RICA)

La producción nacional de los programas de computación, el uso de software importado y el incuestionable impacto de la informática en la sociedad costarricense actual, reclaman una respuesta precisa de carácter jurídico, que proteja esta importantísima y floreciente actividad económica, fomentando su desarrollo y resguardando nuestra soberanía.

El problema de la protección de los programas, como verdaderos bienes (inmateriales), potencialmente susceptibles de apropiación y en todo caso, fuente de inversiones considerables, amerita una consideración específica.

El derecho costarricense protege jurídicamente el «soporte lógico» por la vía del Derecho de Autor. Nuestra Constitución Política, promulgada el 7 de noviembre de 1949, dispone en su artículo 45 que la propiedad es inviola-

ble y a nadie puede privarse de la suya si no es por interés público legalmente comprobado, previa indemnización conforme a la ley. Lo anterior es reforzado por el numeral 47 que señala: «Todo autor, inventor, productor o comerciante gozará temporalmente de la propiedad exclusiva de su obra, invención, marca o nombre comercial, con arreglo a la ley».

La Ley de Patentes de Invención, dibujos y modelos industriales y modelos de utilidad, número seis mil ochocientos sesenta y siete del 25 de abril de 1983, establece claramente que los programas de computación no se consideran invenciones para efectos de esta ley (art. 1, inciso 3, a). La Ley de Derechos de Autor y Derechos Conexos, número seis mil seiscientos ochenta y tres del catorce de octubre de mil novecientos ochenta y dos, regula la materia, estableciendo que las producciones intelectuales confieren a sus autores los derechos a que se refiere esta ley, siendo los mismos titulares de derechos patrimoniales y morales sobre sus obras literarias y artísticas. (art. 1).

Se protegen por su medio las obras de autores costarricenses, domiciliados o no en el territorio nacional, y las de autores extranjeros domiciliados en el país. (art. 2).

Las obras de autores extranjeros, domiciliados en el exterior, gozan en Costa Rica de la protección que les acuerden las convenciones internacionales a que el país se adhiera. (art. 3).

Independientemente de sus derechos patrimoniales, incluso después de su cesión, el autor conserva sobre la obra un derecho personalísimo, inalienable e irrenunciable y perpetuo, denominado derecho moral. (art. 13).

Los artículos 95 a 116 de esta Ley dieron nacimiento al Registro Nacional de Derechos de Autor y Conexos, adscrito al Registro Público de la Propiedad.

Para inscribir un programa de computación, actualmente, es menester presentar una solicitud escrita dirigida al Director del RNDA, en papel de oficio, con doscientos cincuenta colones en timbres fiscales, veinte colones en timbres del Colegio de Abogados y debidamente autenticada, con dos pliegos de papel de oficio en blanco, especificando: a.– Nombre completo, calidades y domicilio del solicitante, si actúa en nombre propio o en representación de alguien, en cuyo caso deberá acompañar certificación de esto e indicar el nombre y domicilio del representado, indicando apartado postal y teléfono. b.– Nombre del programa. c.– Descripción del contenido del programa (Resumen). d.– Copia del programa (en diskete).

Administrativamente se dispuso que sea el programa fuente. e.– Copias de los manuales, firmados por el autor y autenticados. Si los manuales fueren impresos deberán depositarse seis ejemplares para: Biblioteca Nacional, Biblioteca de la Universidad Nacional, Bibilioteca de la Universidad de Costa Rica, Biblioteca del Ministerio de Justicia, Biblioteca de la Asamblea Legis-

lativa y el Registro Nacional de Derechos de Autor y Derechos Conexos. Los respectivos comprobantes de tales depósitos deben adjuntarse a la solicitud.

Una vez presentada la solicitud, el Registrador la revisa y de estar en forma, expide un edicto para su publicación en el Diario Oficial, confiriendo un plazo de treinta días hábiles para oír oposiciones, vencido el cual –de no existir tales– se procede a la inscripción, emitiendo la correspondiente certificación.

La Ley de Derechos de Autor y Derechos Conexos, establece sanciones de carácter penal, para garantizar la efectiva protección de las obras por ella amparadas:

De uno a tres años de prisión al que viole cualquier determinación de la misma, cuando el delito no sea penado específicamente con otra pena. (art. 117, inciso c).

De ocho a doce meses al que: reproduzca una obra literaria o artística protegida, sin la autorización del autor. (art. 119, inciso b); venda, distribuya, guarde en depósito, importe o exporte ejemplares fraudulentamente reproducidos, o de otra forma concurra en la defraudación del autor, del artista, del productor de fonogramas o del organismo de radiodifusión. (art. 119, inciso h).

Sin embargo, es necesario considerar que si bien no resulta lícito alegar que el cassette que reproduce sin autorización un disco, o las fotocopias de un libro, son copias de respaldo, en tratándose de materia informática, es absolutamente necesario realizar y poseer copias de respaldo de los programas, también denominadas copias de apoyo. Back up en inglés. En este sentido se debe regular con claridad la facultad del comprador del soporte lógico para realizar copias de apoyo para su archivo y uso personal.

Independientemente de que nuestro ordenamiento jurídico llegue a contar con un Código Informático, en donde se regulen una serie de aspectos atinentes a la informática como objeto del derecho, es indispensable reformar nuestra estructura normativa de inmediato, para tutelar muchos fenómenos actuales que se encuentran desprotegidos o deficientemente cubiertos, como lo es el soporte lógico, con el afán de proteger la creatividad de nuestros informáticos. Actualmente existen tres propuestas para regular lo atinente a la protección jurídica del «software» en nuestro país.

1.– Proyecto de Ley de Creación del Registro de Programas Informáticos. (julio de 1990).

Introduce la definición de «programa de computadora» como la expresión de un conjunto organizado de instrucciones en lenguaje natural o codificado, contenida en un soporte físico de cualquier naturaleza, de empleo necesario en máquinas automáticas de tratamiento de información, dispositivos, instrumentos o equipos periféricos, en los que se utilice la técnica digital, para hacerlos funcionar de un modo específico y con fines determinados.

Los derechos derivados de esta ley serían independientes del Registro de los programas, siendo los mismos atribuíbles a los extranjeros domiciliados en el exterior, quienes de este modo quedan asegurados de la misma forma que los de los nacionales, desde el momento en que el país de origen del programa conceda, a los nacionales y extranjeros domiciliados en Costa Rica, derechos equivalentes en extensión y duración, a los establecidos en esta ley.

Como requisitos para la inscripción se establecen: a) Que no esté registrado o en proceso de inscripción un programa similar o igual al que se pretende proteger. b) Que el «interface» con el usuario no sea similar o igual al de un programa ya inscrito o en proceso de inscripción. c) Presentar una copia del programa, igual a la que será o es objeto de comercialización. ch) Presentar un manual de instrucciones sobre el funcionamiento del programa, con su respectiva documentación. d) Presentar una declaración jurada sobre el contenido y alcance del programa.

Lo anterior no introduce reformas sustanciales a los requisitos exigidos por la legislación vigente. En cuanto a la definición de las conductas punibles, tenemos que: Incurrirá en la violación de los derechos de propiedad intelectual y será responsable civil y penalmente, con las mismas penas establecidas por la Ley de derechos de autor, el que voluntaria o involuntariamente incurra en:

a) Reproducción o uso ilegítimo del programa o material de apoyo, a excepción de ser indispensable para la utilización del programa.

Esta excepción constituye en nuestro criterio un importante avance, ya que como se apuntó anteriormente, en materia informática es no sólo deseable sino necesario para el usuario contar con copias de apoyo de los respectivos programas.

b) Citas parciales para fines no didácticos sin que las acredite el autor del programa.

c) Citas totales o parciales sin permiso del autor del programa.

ch) Semejanza de un programa con otro, salvo que fuese por las características funcionales de su aplicación, de la observancia de preceptos legales, reglamentarios, de normas técnicas o la existencia de limitaciones sobre su forma de expresión.

Todas las anteriores violaciones conllevarán una pena de prisión de tres a doce meses.

2) Proyecto presentado por algunos vendedores de software.

Plantea la reforma de los artículos 1, 7, 16, 41, 74, 89, 94, 97, 103, 106, 114 y 125 de la Ley de Derechos de Autor y Derechos Conexos No.6683 y sus reformas.

Por obra se entenderá cualquier creación del intelecto humano en las ramas: artística, literaria, científica y los programas de computación. De este modo se pretende asegurar la inclusión del software bajo el amparo de la Ley de Derechos de Autor.

Tratándose de programas de computación, únicamente se permitirá el uso de la reproducción final para usos informativos. No se permitirá acceso a la información, ni se permitirá la duplicación en que se presente la obra final, ni se expedirán copias, salvo que quien las solicite se acredite como su autor, su licenciatario o causahabiente, tenga autorización expresa del autor o así lo ordene resolución judicial. Se entiende por reproducción final el manual de operaciones y su grabación en cualquier medio electromagnético o electrónico.

Para inscribir una producción, el interesado presentará, ante el Registrador, una solicitud escrita con los siguientes requisitos, que tampoco difieren de los enumerados por la ley vigente: 1) Nombre, apellidos y domicilio del solicitante, indicando si actúa en nombre propio o en representación de alguien, en cuyo caso deberá acompañar certificación de esto e indicar el nombre, apellidos y domicilio del representado. 2) Nombre, apellidos y domicilio del autor y editor y del impresor, así como sus calidades. 3) En el caso de programas de computación, se presentarán los manuales de operación y su grabación en cualquier medio electromagnético o electrónico y las pantallas básicas que identifican al programa.

3) Nuestra propuesta de reforma al Derecho autoral

Proponemos que se discuta una reforma al Derecho Autoral costarricense, incorporando la normativa específica atinente al «Soporte Lógico» en la LEY DE DERECHOS DE AUTOR Y DERECHOS CONEXOS (6683 DEL 14 DE OCTUBRE DE 1982).

Es conveniente incluir en las normas que corresponda, junto a los conceptos «obra literaria y artística» el de «soporte lógico», pues el mismo corresponde a una nueva categoría de la creatividad humana, distinta de las dos anteriores, que sólo lo englobarían mediante un proceso analógico librado en buena parte al arbitrio de los registradores.

Por la novedad del término, será necesario incluir en el texto legal la definición del mismo: «Por «soporte lógico» debe entenderse el conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de que un «ordenador» –un aparato electrónico o similar capaz de elaborar informaciones– ejecuta determinada tarea u obtenga determinado resultado. Quedan expresamente excluidos de esta protección los lenguajes de programación y los algoritmos.»

La exclusión se justifica en razón de que ambos son de uso general y no son obra del autor del soporte lógico que se desea proteger.

Habiéndose ampliado de esta manera el radio de aplicación de la Ley de comentario, es menester que en ella se incorpore un capítulo específico, denominado «Soporte Lógico», por las particulares relaciones que a partir suyo se pueden dar.

CAPITULO VII BIS

SOPORTE LOGICO

Artículo 57 bis.– El autor de un soporte lógico es la persona física o grupo de personas físicas que lo han creado.

A menos que se disponga lo contrario por contrato:

a.– Con respecto a los soportes lógicos creados por un grupo de personas físicas, el derecho exclusivo será ejercido en común.

b.– Cuando un soporte lógico sea creado bajo un contrato, la persona física o jurídica que lo encargue estará facultada para ejercer todos los derechos respecto de éste.

c.– Cuando un soporte lógico sea creado en el curso de una relación laboral, el empleador estará facultado para ejercer todos los derechos respecto del programa.

d.– Respecto de soportes lógicos que sean generados mediante el uso de programas de computación, la persona física o jurídica que dé origen a la generación de programas subsecuentes deberá estar facultado para ejercer todos los derechos respecto de estos programas.

e.– El usuario del soporte lógico solo está autorizado para realizar modificaciones o adaptaciones a éste que tiendan a la adecuada utilización en su computador o al aumento de su eficacia.

f.– Los propietarios de copias de soporte lógico legítimamente adquiridas, podrán poseer hasta dos copias adicionales de respaldo para su exclusivo uso personal, siempre y cuando sean indispensables para la utilización del equipo del usuario.

Dentro de los requisitos de inscripción, es necesario indicar que en el caso de soporte lógico, será indispensable aportar reproducción fiel y exacta en medio electromagnético correspondiente al programa, que será o es objeto de comercialización, manual del usuario, copias impresas de las principales pantallas y una descripción suscinta sobre el contenido y alcance del programa. En tratándose de soporte lógico solo se presentará un ejemplar de los programas y documentos requeridos ante el Registro correspondiente.

Cuando se denieguen inscripciones, en el caso de obras científicas y de soporte lógico, el recurso administrativo de apelación será planteado no ante el Ministro de Cultura, Juventud y Deportes, sino que será sustanciado por

el Ministro de Ciencia y Tecnología. Al listarse las obras cuya ilegítima reproducción se encuentra protegida, deberá incluirse dentro de éstas al soporte lógico, cosa harto necesaria ya que debemos recordar que no puede imponerse una sanción en base a consideraciones analógicas.

Por último, para garantizar una debida salvaguarda del soporte lógico, será necesario tipificar, como conductas sancionadas con prisión de ocho a doce meses (artículo 119 de la Ley de Derechos de Autor), los supuestos de divulgación, entrega a terceros y uso sin autorización de una copia de respaldo y de elaboración, importación, posesión, uso o comercialización de artículos o soportes lógicos destinados a facilitar la remoción o elusión de cualquier medio técnico que pueda haber sido aplicado para proteger los programas.

De este modo, la adecuada reforma del texto vigente garantizaría la efectiva protección del soporte lógico, como respuesta al avance tecnológico que caracteriza nuestro tiempo, sin necesidad de promulgar una Ley específica sobre la materia.

El derecho informático en el proyecto de acuerdo TRIPs de la Rueda Uruguay

CARLOS M. CORREA

Abogado. Licenciado en Economía. Director de la Revista del Derecho Industrial. Coordinador Regional del Programa PNUD (ONUDI) de Cooperación en Informática y Microelectrónica. Director de la Maestría en Política y Gestión de la Ciencia y la Tecnología de la Univ. de Buenos Aires.

(ARGENTINA)

1. EL PROYECTO DE ACUERDO TRIPs

En diciembre de 1991, el Secretario General del GATT sometió a los países miembros de esa organización una ambiciosa propuesta global de acuerdo multilateral para regular diversas facetas del comercio internacional. Tal propuesta incluyó –por primera vez en el historia del GATT– normas relativas a propiedad intelectual, contendidas en un proyecto de acuerdo sobre «Trade related aspects of intellectual property rights» (TRIPs).

El proyecto de acuerdo TRIPs, en caso de ser finalmente aprobado, influirá de manera sustancial en múltiples aspectos de la propiedad intelectual, por tres razones principales.

En primer lugar, dicho proyecto contiene normas que serán aplicables de manera uniforme en más de cien países miembros del GATT. Desde que ellas están formuladas como standards mínimos, su instrumentación asegurará un cierto «piso» en la protección de los derechos intelectuales en casi todo el mundo.

Segundo, el Acuerdo será el más comprensivo entre los convenios internacionales sobre la materia, pues incluye disposiciones sobre derechos de autor (y derecho vecinos), diseños industriales, marcas, indicaciones de origen, patentes, diseño de circuitos integrados e información confidencial. Los únicos títulos no abordados –sino de modo marginal– han sido los derechos de obtentor y los modelos de utilidad.

Tercero, la adpoción de TRIPs permitirá a cualquier país miembro del GATT acudir al sistema de resolución de controversias del GATT y, en su caso, aplicar represalias comerciales en cualquier rubro de bienes o servicios si se determina la inobservancia de alguno de los standards mínimos de protección.

El proyecto de Acuerdo no establece distinción entre las normas aplicables a países desarrollados y en desarrollo, excepto en lo que respecta a la fecha de entrada en vigor de las nuevas disposiciones (normas transitorias).

En materia de derecho informático, el Acuerdo TRIPs contiene disposiciones que afectan tres temas claves que se tratan sucesivamente más abajo, en relación con la protección de a) los programas de computación; b) los bancos de datos, y c) los circuitos integrados.

2. LA PROTECCION DEL SOFTWARE

a) La situación actual

La definición de standards internacionales de protección mínima para el software ha sido, sin duda, uno de los objetivos importantes de los países que han impulsado la negociación de un Acuerdo sobre TRIPs. Si bien en la última década numerosos países desarrollados y en desarrollo han adoptado el derecho de autor como forma principal de protección (Correa, 1990a), diversos problemas no han encontrado una solución plena, particularmente en la perspectiva de la industria de software con una vasta acción internacional.

Primero, no todos los países han resuelto definitivamente la cuestión del régimen legal aplicable al software. En algunos, la cuestión sigue irresuelta (p. ej. Tailandia), en tanto en otros (varios países de América Latina), la jurisprudencia aún es frágil y no ha habido cambios legislativos que introduzcan de manera explícita tal protección[1].

Segundo, aún en países en donde la aplicación del derecho de autor ha sido admitida en principio, existen dificultades de «enforcement» debido a la naturaleza de los procesos judiciales o a la escasa significación de las penas. La «piratería», más controlada hoy que hace diez años, no ha dejado sin

[1] Sólo Brasil, México y Chile cuentan con normas legales recientes que clarifican la aplicación del derecho de autor a los programas de computación. Se han dictado también decretos en tal sentido en Colombia y Uruguay (CORREA, 1991).

embargo de constituir un fenómeno extendido, incluso en países industrializados.

Tercero, diferencias en los regímenes nacionales de derecho de autor condujeron a resultados prácticos disímiles. El ejemplo más notable, tal vez, es el de la interpretación restrictiva del concepto de «originalidad» en el derecho alemán (y suizo), con la consecuente desprotección de una gran parte del software protegible en otros países bajo un concepto más elástico (basado en la existencia de un esfuerzo intelectual).

Cuarto, la dicotomía idea/expresión ha resultado de compleja aplicación en relación con una obra funcional como el software y la extensión de la protección suscita diferencias entre países. Así, en tanto en Japón y los Estados Unidos la ingeniería inversa tendería a ser aceptada (Pilny, 1992), en los países miembros de la CEE –sobre la base de la reciente Directiva sobre la Protección de los Programas de Computación[2] – ella sólo es admisible para la inetopreabilidad de un programa creado de manera independiente (artículo 6).

Quinto, las diferencias de interpretación sobre el alcance de los derechos se han manifestado incluso en el sistema judicial de los Estados Unidos. La citada decisión en Whelan vs. Jaslow (1986, U.S. Court Of Appeals, Third Circuit) que admitió la protección de la estructura y organización de un programa ha sido recientemente revertida en Computer Associates vs. Altai (junio de 1992, U.S. Court of Appeals, Second Circuit).

Sexto, y por último, si bien se admite en general la protección del programa-objeto como un «trade secret», una forma adicional de protección puede basarse en el sistema de patentes. Al menos en los Estados Unidos, la solicitud de patentes respecto de programas de computación ha comenzado a constituir una tendencia visible, la que se acentuará quizás en la medida que persista la incertidumbre en relación con el alcance de la protección vía copyright (Business Week, 1992, p. 49).

b) Las reglas de TRIPs

I) Protección como obra literaria

El proyecto de Acuerdo TRIPs (artículo 9.1) obliga a la observancia de los artículos 1 a 21 y del Apéndice de la Convención de Berna, en su versión de 1971. Si bien tal Convención no hace referencia expresa a los programas de computación, ha prevalecido en general el criterio de que ellos están amparados por sus disposiciones[3]. Para evitar toda duda, el artículo 10 de dicho proyecto de Acuerdo establece que los «computer programs, whether in

[2] Directiva del Consejo 91/250/CEE del 14-5-1991.

[3] En tal sentido, el «Protocolo» a la Convención de Berna bajo consideración en el ámbito de la OMPI, no haría sino hacer explícita dicha cobertura (ver OMPI, 1992).

source or object code, shall be protected as literary works under the Berne Convention (1971)».

La norma citada no sólo representa un punto final a cualquier especulación sobre la aplicación del Convenio al software de Berna. Ella zanja también la cuestión –debatida en la doctrina y jurisprudencia– de la categoría de obra intelectual a la que pertenecen o se equiparan los programas de computación[4]. Ellos deben ser protegidos «como» obras literarias, lo que implica descartar soluciones que como, la de la ley francesa de 1986, se basan en la equiparación de hecho del software a obras de arte aplicadas con sujeción a un plazo menor de protección (veinticinco años).

II) Alcance de la protección.

En la propuesta del Japón al grupo negociador de TRIPs –en línea con la legislación de aquel país– el artículo 10.1 referido se completaba con la aclaración de que «such protection shall not extend to ideas, procedures, methods of operation or mathematical concepts». El propósito de este agregado era trazar una línea demarcatoria más clara entre lo que debe entenderse como apropiable y lo que no debe caer bajo el derecho de propiedad, demarcación que tiene particular importancia a la hora de juzgar la legitimidad de la ingeniería inversa y la posibilidad de imitar la estructura interna y organización de un programa.

Si bien la propuesta referida no encontró consenso, un texto similar al indicado se incorporó en el artículo 9.2 del proyecto de Acuerdo más con un alcance que se extiende a todos los derechos amparados bajo la Convención de Berna y no sólo a los programas de computación. Dicho artículo establece que «Copyright protection shall extend to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such». La expresión «as such» de este artículo in fine puede introducir un sesgo restrictivo en la interpretación de la norma que no estaba presente en la propuesta japonesa.

Otra norma relevante para juzgar la extensión de los derechos, pero también de alcance general, está contenida en el artículo 13, de conformidad con el cual «PARTIES shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder».

La admisibilidad o no de la descompilación e ingeniería inversa de los programas de computación, así como la extensión de la protección más allá de la expresión (incluyendo a la estructura interna) dependerá de la interpretación que las legislaciones nacionales brinden a las normas indicadas. En todo caso, es claro que el proyecto de Acuerdo ha eludido resolver de manera

[4] La controversia al respecto se centró principalmente en la posibilidad de reconocer carácter de obra literaria a un programa no legible por el hombre, por ejemplo, incorporado en una memoria ROM.

precisa esos aspectos, con lo cual su poder armonizador en esa materia será limitado.

III) Derechos de alquiler.

El artículo 11 del proyecto comentado introduce, por primera vez en un tratado multilateral[5], la noción de «rental rights» (derechos de alquiler) como uno de los elementos del haz de derechos exclusivos del titular de un programa de computación. Según dicho artículo «In respect of at least computer programs and cinematographic works, a Party shall provide authors and their successors in title the right to authorise or prohibit the commercial rental to the public of originals or copies of their copyright works...In respect of computer programs, this obligation does not apply to rentals where the program itself is not the essential object of the rental».

El reconocimiento de los derechos de alquiler no admite excepciones –a diferencia de lo que el proyecto de Acuerdo prevé para la obras cinematográficas–, si bien se aclara su inaplicabilidad en el caso de que el software sea parte no esencial de otro producto alquilado (p. ej. un automóvil). El reconocimiento expreso de tales derechos parece tener particular importancia en los regímenes basados en el concepto de «copyright» mas no para aquellas legislaciones –como las inspiradas en el derecho continental– que típicamente otorgan al autor un derecho exclusivo de distribución.

IV) Duración.

En materia de duración de la protección, el Acuerdo TRIPs puede tener un importante efecto armonizador de las legislaciones nacionales con relación a las obras que no pertenecen a personas físicas. En el caso del software, lo más frecuente es que los programas comercializados (particularmente los de tipo «standard») sean desarrollados por empresas u otras entidades, a quienes la ley atribuye –directa o indirectamente– la titularidad de aquéllos.

Según el artículo 12 del proyecto de Acuerdo, las obras –excepto las fotográgicas y de arte aplicado– tendrán una tutela no inferior a cincuenta años contados desde el fin del año de su publicación y, en ausencia de ésta dentro de los cincuenta años desde la creación, cincuenta años contados desde el fin del año de publicación.

V) Otros aspectos.

Como se señaló más arriba, el patentamiento del software puede convertirse en una alternativa o complemento a la protección vía derecho de autor. El Acuerdo de TRIPs –a diferencia de la Convención Europea de patentes y de diversas legislaciones– no excluyen la posibilidad de que el software sea

[5] El único antecedente importante de esta disposición se encuentra en la ya mencionada Directiva de la CEE de mayo de 1991 (artículo 4 c). En el plano nacional, se destaca la «Computer Software Rental Amendments Act» de 1990 de los Estados Unidos.

patentado. De acuerdo con el artículo 27.1 «patents shall be available for any inventions, whether products or procesess, in all fields of technology...».

Por otra parte, tal Acuerdo daría nacimiento al primer cuerpo internacional de normas sobre «undisclosed information», una forma de protección de particular importancia para los programas de computación comercializados exclusivamente en su modalidad de programa-objeto. La sección 7 contempla la aplicación de la disciplina de la competencia desleal, sobre la base de definiciones y reglas inspiradas en la legislación estadounidense sobre «trade secrets».

Diversas disposiciones de la Parte III del Acuerdo –que no se analizan aquí– sobre el ejercicio y «enforcement» de los derechos de propiedad intelectual pueden ser de relevancia para la protección del software en su faz práctica. Así, por ejemplo, el artículo 51 faculta a detener en las aduanas «pirated copyright goods», en tanto el artículo 61 obliga a los países miembros del GATT a disponer de procedimientos y sanciones penales para la «piratería de copyright en escala comercial»

3. COMPILACIONES DE DATOS

El artículo 10.2 del proyecto de Acuerdo dispone:

«Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall be without prejudice to any copyright subsisting in the data or material itself».

La emergente industria de bancos de datos y la creciente importancia económica de éstos, han generado demandas por una protección más explícita y efectiva de aquéllos, tanto en lo que respecta a la reproducción y distribución de la información compilada como a la extracción o re-utilización no autorizada del contenido de un banco de datos.

Si bien algunas legislaciones, como la de los Estados Unidos (artículo 103 de la U.S. Copyright Act) y del Japón (Ley 64 de 1986)[6] prevén la protección de las compilaciones de datos en cuanto tales, la Convención de Berna sólo se refiere a la de «colecciones de obras literarias o artísticas tales como enciclopedias y antologías». En el ámbito de la CEE se ha elaborado una propuesta de Directiva para la «Protección Legal de las Bases de Datos» con base en el derecho de autor[7], mas limitada a aquéllas operadas por medios electrónicos y a los derechos económicos de los titulares. Además del típico derecho a impedir la reproducción no autorizada, dicha propuesta

[6] Con relación a la legislación japonesa, ver KARJALA (1986).

[7] El «Green Paper» sobre propiedad intelectual de la Comisión de las Comunidades Europeas había sugerido, en 1988, la posibilidad de desarrollar un régimen sui generis de protección de las bases de datos (ver CLARK, 1991).

prevé un «derecho especial» para prevenir la extracción o re-uso no autorizado, del total o una parte sustancial, de la información almacenada.

Según se desprende del citado artículo 10.2 del proyecto de Acuerdo, las negociaciones en TRIPs concluyeron con un texto que, por un lado, suplementa la Convención de Berna en tanto alude a compilaciones «de datos» y no sólo a la de obras autorales y que, por el otro, no se limita a las bases de datos computarizadas, sino que abarca también las manuales. A diferencia de la propuesta de Directiva de la CEE, además, la elaborada en TRIPs no incluye referencia alguna a «derechos especiales» para evitar la extracción o re-utilización de datos.

Con el alcance expuesto, el proyecto de Acuerdo claramente inscribe la protección de las compilaciones de datos en el ámbito del copyright y en el marco de los derechos exclusivos que típicamente se reconoce bajo aquel régimen. La cobertura de las compilaciones sea que ellas fueren computarizadas o manuales justifica, por cierto, que no se fuere más lejos en cuanto a los derechos reconocidos, sin perjuicio de la posibilidad, para cualquier país, de conceder una protección adicional (como la propuesta en la CEE).

4. CIRCUITOS INTEGRADOS

La protección del diseño (o «layout») de los circuitos integrados está dando lugar a una situación sin precedentes en el dominio de la propiedad intelectual. Tras cerca de cinco años de negociaciones, la Conferencia Diplomática de Washington adoptó, en mayo de 1989, un Tratado para la protección de dichos diseños –vía una modalidad sui generis– por una abrumadora mayoría de los países participantes. Estados Unidos y Japón, principales productores mundiales de semiconductores e interesados en el establecimiento de tal protección, no suscribieron el texto del Tratado acordado[8].

El proyecto de Acuerdo TRIPs, como se ha visto, suplementa la Convención de Berna en diversos aspectos (también lo hace con las Convenciones de Roma y París). En el caso de los circuitos integrados, y aún cuando el Convenio de Washington no está en vigor, dicho proyecto obliga a los países miembros a observar sus disposiciones con las salvedades y agregados que –no sorprendentemente– reflejan las objeciones de los Estados Unidos y el Japón a dicho Tratado.

En primer lugar, el referido proyecto de Acuerdo incluye una norma que fue explícitamente rechazada en la Conferencia de Washington por los países en desarrollo, en virtud de la cual el ámbito de la protección no sólo se extiende a los diseños y a los circuitos integrados que los incorporan, sino a

[8] Sobre estas negociaciones y las implicaciones del Tratado de Washington, ver CORREA (1990b) y KITAGAWA (1992).

los artículos que incorporan tales circuitos «en la medida que continue conteniendo un diseño ilegalmente reproducido» (artículo 36).

Segundo, se prevé la excepción del «infractor inocente». No se considerará infractor a quien adquiriere un circuito integrado o un artículo que incorpore un diseño reproducido ilegalmente sin conocer ni tener razonables fundamentos para conocer de tal reproducción ilegítima. El artículo 37.1 del proyecto de Acuerdo agrega, sin embargo, que «after the time that such person has received sufficient notice that the layout-design was unlawfully reproduced, he may perform any of the acts with respect to the stock on hand or ordered before such time, but shall be liable to pay to the holder of the right a sum equivalent to a reasonable royalty such as would be payable under a freely negotiated license in respect6 of such a layout-design».

El pago de una regalía por el infractor inocente fue, en la Conferencia Diplomática de Washington, uno de los puntos más objetados, debido a la imposibilidad que tienen adquirentes de los más diversos productos industriales, particularmente en los países en desarrollo, de verificar la legitimidad de los diseños incorporados en los «chips». La solución adoptada por el proyecto de Acuerdo puede constituirse, en la práctica, en una barrera al comercio y en una amenaza permanente sobre los compradores de bienes electrónicos y otros que incorporan componentes informáticos. Lo lógico y justo sería, en todo caso, que la acción del titular del diseño se dirija contra el fabricante del producto que lo incorpora y no contra quien lo adquiere (salvo que lo hiciera de mala fe).

Tercero, el artículo 37.1 hace aplicables a las licencias obligatorias de diseños de circuitos integrados (uno de los puntos de discordia para los Estados Unidos en el Tratado de Washington) las detalladas disposiciones que el proyecto de Acuerdo contiene sobre «otros usos» (no autorizados por el titular) de las patentes de invención. Ello implica, entre otros aspectos, la necesidad de una negociación previa con el titular y la evaluación de caso por caso de las solicitudes de licencia.

Por último, en tanto el Tratado aludido estableció una duración mínima de los derechos de ocho años, el proyecto de Acuerdo extiende tal plazo a diez años.

5. PRINCIPALES CONCLUSIONES

El análisis efectuado permite extraer las siguientes conclusiones principales.

La aprobación del Acuerdo TRIPs significará un paso importante en la universalización del ya predominante patrón legislativo basado en la aplicación del derecho de autor para la protección del software y en la consideración de éste como obra literaria. Las normas alcanzadas amplían y refuerzan los derechos para combatir la copia ilegítima («piratería») de programas de

computación en los países en que el marco normativo es aún frágil o impreciso. En cambio, el Acuerdo no aportará soluciones y criterios uniformes para los aspectos tan cruciales como controvertidos relacionados con la extensión de la protección y la admisibilidad de la ingeniería inversa. No es difícil presumir que estos vacíos son el resultado de la complejidad de los temas a ser abordados y de las significativas divergencias que, según se observó más arriba, separan incluso a la jurisprudencia en los Estados Unidos.

En materia de compilaciones de datos, el proyecto de Acuerdo ofrece la posibilidad de universalizar su protección vía el derecho autoral –con lo que se excluye la vía de un régimen sui generis–. Si bien deja igualmente sin resolver aspectos vinculados con actos diferentes a la reproducción, tal como la extracción y re-utilización de los datos, la solución parece la más adecuada dada la amplia cobertura de la norma propuesta (bases de datos computarizadas y manuales) y la dificultad existente para trazar la línea divisoria entre lo que es protegible y lo que no lo es.

En lo que respecta a diseños de circuitos integrados, las modificaciones y complementos introducidos al Tratado de Washington reflejan, por un lado, la pérdida de capacidad negociadora que, en corto término, sufrieron los países en desarrollo (y los que coincidieron con ellos en la Conferencia de Washington) al pasar el tema del ámbito de la OMPI al del GATT. Por el otro, tales cambios no representan una mejora de las normas multilaterales sobre la materia y pueden, particularmente, afectar indebidamente a los adquirentes de bienes que incorporan «chips».

Como conclusión general, el proyecto de Acuerdo TRIPs influirá ciertamente en la configuración de componentes importantes del derecho informático en un gran número de países. En el área del software, la mayor influencia se dará en los países en desarrollo que aún no hubieren definido claramente su protección vía derecho de autor. En los otros dos temas tratados, la influencia será aún más abarcativa pues el proyecto introduce soluciones que son nuevas o que significan una definición más firme a la existente en la actualidad tanto en países industrializados como en desarrollo.

Sin perjuicio de ello, no puede verse al proyecto de Acuerdo comentado como el punto final a los debates y diferencias que aún prevalecen en relación con múltiples temas de la propiedad intelectual en el área de la informática. Si bien tal proyecto define la modalidad y ciertos contenidos de la protección son múltiples los aspectos que separarán aún a las empresas –según sus posiciones relativas en el mercado y su capacidad tecnológica–, a los expertos y a los países con distintos grados de desarrollo y percepciones sobre el modo de favorecer la producción y el comercio de bienes informáticos.

REFERENCIAS BIBLIOGRAFICAS

BUSINESS WEEK (1992), «Bit by bit, software protection is eroding», Julio 20, pp.49-50.

CLARK, C. (1991), «The value of information –The protection of compilations, including databases», Managing Intellectual Property, noviembre, pp. 10-12.

CORREA, C. (1990), Tecnología y desarrollo de la informática en el contexto Norte-Sur, Eudeba, Buenos Aires, 220 pp.

CORREA, C (1991 a), «Evolución reciente del derecho informático en América Latina», La Ley, Tomo A, Buenos Aires, pp. 848.

CORREA, C. (1991 b), «Intellectual property in the field of integrated circuits: implications for developing countries», World Competition, Geneva, pp. 83-102

KARJALA, D. (1986),«Protection of computer databases under japanese law», European Intellectual Property Review, vol. 8, Nº 9, setiembre, pp.267.

KITAGAWA, Z. (1991), «Treaty on intellectual property in respect of integrated circuits –A failed success–», in Festschrift für Werner Lorenz, Mohr, Tübingen, pp.646-675.

PILNY, K. (1992), «Legal aspects of interfaces and reverse engineering –Protection in Germany, the United States and Japan», IIC, Munich, pp. 196-218.

OMPI (Organización Mundial de la Propiedad Intelectual) (1992), «Cuestiones relativas a un eventual protocolo del Convenio de Berna», Parte I, Ginebra, julio, pp.1-25.

Los Virus Computacionales como medio de Protección del Software

JORGE MIER Y CONCHA SEGURA

Licenciado en Derecho, Asesor en Propiedad Industrial e Intelectual, Inversiones Extranjeras y Derecho del Trabajo.

(MEXICO)

Nadie debe asustarse de lo que piensa aunque su pensar aparezca en pugna con las leyes más elementales de la lógica.

Antonio Machado

VIRUS.–(Del Lat. Virus, Tumor, ponzoña) Bact. partícula ultramicroscópica de nucleoproteína capaz de multiplicarse en ciertas células vivas, y que produce muchas enfermedades en las plantas, los animales y el hombre.[1]

Informática. Es un fragmento de un programa de computación, usualmente unido al principio o al final de un arhivo normal de un programa, que contiene una instrucción que le permite duplicarse a sí mismo o llevar a cabo alteraciones, destrucciones o alguna acción complementaria, en archivos aislados o en discos completos.[2]

I. CUESTIONES PRELIMINARES

Pakistaní, Miguel Angel, Viernes 13, El baile del Diablo; frases, nombres, fechas, lugares, que muy posiblemente usemos a diario, sin embargo,

[1] SELECCIONES DEL READER'S DIGEST, Gran Diccionario Enciclopédico Ilustrado Tomo VIII, México, Edit. Reader's Digest México, 1972.

[2] TYLER,G. –New Technology–. Management Services, Vol. 34, No. 6, 1990, pp. 21-24.

para un programador o usuario de una computadora, su significado real va más allá de la simple literalidad.

Los virus computacionales, parte integrante de lo que comunmente se ha denominado «SOFTWARE ROGUE» (Bribón, Maleante), han logrado, actualmente, infectar por encima de 16.000 computadoras alrededor del mundo, ocasionando pérdidas materiales incalculables.

El Software Rogue, que se define como todo aquel conjunto de instrucciones o dispositivos tendientes a alterar el funcionamiento normal de un sistema computacional, surge en principio por la falta de protección que los programadores sienten de sus creaciones. Mucho antes de los casos de Look and Feel, existía el problema de la piratería, cuyos antecedentes son tan remotos como el software mismo.

La aceptación dentro de los Derechos de Autor de los programas de computación, partió de dos supuestos, el primero referido a que, para las obras autorales, se reducen significativamente los requisitos de protección, siendo simplemente la originalidad y la objetivización (fijación tangible) indispensables, y no así, como en el caso de las figuras protegidas por la Propiedad Industrial, exámenes o cuestionamientos profundos de novedad; y en segundo término, la generalización que a nivel mundial había alcanzado este sistema.

Resulta obvio que un sistema de protección implantado más por comodidad que por conveniencia, fuese superado rápidamente por los avances tecnólogicos, de ahí que, al continuarse con el copiado no autorizado de programas, sus autores buscaran medidas alternas para evitar las reproducciones ilícitas, y obtener la remuneración justa por su trabajo.

Surgieron pues, entre otros, la criptografía, los códigos de acceso, los caballos de Troya, las bombas lógicas, los gusanos y los virus, que con el correr del tiempo fueron aumentando sorpresivamente su capacidad destructiva y reproductiva.

Antecedente de los virus, lo constituye el gusano, software rogue que se caracteriza por trasladarse a través de una red de computadoras reproduciéndose en cada una de las terminales, hasta que la cantidad de memoria que ocupa es tal, que ocasiona la caída o falla del sistema. En principio, el gusano, como los virus, no traía consecuencias destructivas, sino simples molestias, o mensajes tendientes a ridiculizar al usuario por su falta de ética, pero eran fácilmente superables, pues al apagar la máquina, todo efecto desaparecía.

Sin embargo, estas advertencias no cambiaron la mentalidad de los piratas informáticos, quienes en lugar de disminuir sus actividades, las aumentaron, ¿y por qué no?, el hardware se depreciaba con velocidad, aún y cuando su capacidad crecía exponencialmente, mientras que el software aumentaba, momento a momento su valor. Un pirata, a mediados de los ochenta se jac-

taba al mostrar todo lo que había podido conseguir, desde los programas más sencillos hasta los últimos lenguajes, no importando que nunca llegara a utilizarlos, pues la filosofía era «quien más tiene, más sabe». Así, los programadores se vieron forzados a cambiar palabras por acciones, trayendo en consecuencia la malignidad de los virus.

> «Octubre 1987. Una gran cantidad de usuarios de microcomputación de la Universidad de Delaware (E.E.U.U.), han estado reportando problemas relacionados con sus discos de datos. Al mismo tiempo, usuarios del área de acceso general de microcomputación, han tenido graves problemas para correr determinados paquetes de software».
>
> «Diciembre 1987. Un usuario de una computadora personal IBM en Israel se dió cuenta que un programa que había corrido cientos de veces en el pasado, repentinamente había dejado de funcionar ya que era demasiado grande para la capacidad de memoria».

Pequeñas notas periodísticas, como estas, fueron dando aviso de pérdida de información de sistemas, a medida que el uso de los virus fue en aumento, las pequeñas notas pasaron a ser encabezados, como sucedió el pasado 6 de marzo, fecha de ataque del virus conocido como Miguel Angel, en honor del natalicio del gran artista italiano, noticia que ocupó las primeras planas Japón hasta México. Los virus se convirtieron en armas informáticas, la antigua idea de protección degeneró en un virus destructivo; crear no para defenderse, sino para atacar.

El hecho de que el software sea tan fácil de reproducirse, ha favorecido la propagación de los virus, el ingresar información vía MODEM, conectarse con una red, bajar información vía satélite, o utilizar shareware ya implica cierto riesgo de infección.

La amenaza vírica ha superado todas las fronteras, todos los lenguajes e ideologías, creciendo de tal manera, que no hay un solo usuario que aprecie sus archivos, que no tenga fobia a utilizar un programa ajeno, sin pasarlo previamente por un SCAN o bien sin haberlo «vacunado». Hasta cierto grado los virus han cumplido su función, ¡pero a que costo!.

El primer proceso criminal en que se condenó a un programador rogue, dió inicio en mayo de 1988, cuando la compañía de valores UPSA e IRA Co., ubicada en Fort Worth, Texas, Estados Unidos, demandó a su antiguo oficial de seguridad informática, Donald Gene Burleson, acusándolo de haber ingresado en los sistemas de la empresa un virus que ocasionó la pérdida de más de 168.000 registros de ventas. Se comprobó que El Sr. Burleson activó el virus, dos días antes de ser despedido, lo que le valió una condena de 7 años de prisión y pago de una indemnización a favor de la empresa de 12.000 dlls US.

A este caso siguieron varios en el mismo sentido, entre los más discutidos, pues fue el primero que transgredió las barreras estatales e ingresó al ámbito federal de justicia de Estados Unidos, el de Robert T. Morris Jr., un

universitario de 23 años, que creó un Gusano que se extendió por varias universidades americanas hasta llegar a penetrar los archivos de la NASA. Increiblemente en un lapso de 36 horas, contagió más de 6000 computadoras. El culpable, aunque actuó con negligencia, enfrentó una sentencia de 5 años de prisión y multa de $250,000 dlls US.

En ambos casos las leyes que se aplicaron tenían menos de tres años de vigencia.

La mayoría de los países latinoamericanos, en esta época de apertura de mercados, se enfrenta a un grave problema, pues los órganos judiciales carecen de la preparación suficiente para desentrañar los efectos y alcances que pueden traer consigo los delitos informáticos. El caso mexicano sirve de claro ejemplo para demostrar lo sustentado con anterioridad, pues en vísperas de la celebración del Tratado de Libre Comercio y de las reformas a la Ley de Inversiones Extranjeras, la apertura económica y el ingreso de capitales frescos del exterior se hace inminente. No obstante, la euforia de su firma nos hace olvidar los problemas legales que enfrentaremos, sobre todo con los Estados Unidos de América, pues su sistema legal, mucho más flexible que el nuestro, plantea serias penas, como ya se mencionó, a algunos delitos informáticos, mismos que las leyes mexicanas ignoran. Dentro de las bases que conforman el Tratado Trilateral de Referencia, se establece una especial protección a las figuras que contemplan los derechos intelectuales, muy particularmente a los programas de cómputo y circuitos integrados, manteniendo, sin embargo, a los primeros en el ámbito de protección autoral.

Abordaré el problema de los virus desde diferentes puntos de vista, a fin de poder tener una visión global del problema, a sabida cuenta que los factores sociales y económicos no se separan jamás del derecho, pues este es resultado de la realidad en que se vive, del Aquí y Ahora.

II. DESDE EL PUNTO DE VISTA DEL DERECHO DE AUTOR

¿Qué pasa con los virus en la legislación mexicana?. La Constitución Política de los Estados Unidos Mexicanos, consagra el Derecho de Autor, en su artículo 28 al decir:

> «...Tampoco constituyen monopolios los privilegios que por determinado tiempo se concedan a los autores y artistas para la producción de sus obras y los que para el uso exclusivo de sus inventos, se otorguen a los inventores y perfeccionadores de alguna mejora».

El artículo séptimo de la misma regulación, añade que:

> «...Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública...».

El art. 19 de la Ley Federal de Derechos de Autor vigente, complementa los artículos anteriormente citados al decir:

«El registro de una obra intelectual o artística no podrá negarse ni suspenderse bajo el supuesto de ser contraria a la moral, al respeto a la vida privada o al orden público, sino por sentencia judicial, pero si la obra contraviene las disposiciones del código penal o las contenidas en la Convención para la Represión del Tráfico y Circulación de Publicaciones Obscenas, la Dirección General del Derecho de Autor lo hará del conocimiento del Ministerio Público para que proceda conforme a la ley».

De la lectura de los preceptos anteriores, se desprende que los virus, independientemente de su finalidad o función, por el solo hecho de ser obras se encuentran bajo la tutela del Derecho de autor.

III. DESDE EL PUNTO DE VISTA DEL DERECHO PENAL

Un enorme problema radica en que, un gran porcentaje de las legislaciones mundiales, no contemplan dentro de sus códigos respectivos a los delitos informáticos, siendo, hasta el año pasado, los más actualizados, los países del Common Law o Derecho Común. A pesar de ello, basándose en el viejo principio de derecho penal que dice: *«Nullum crimen, nulla poena sine lege»,* poco se ha podido hacer, ya que por más que se intente identificar ciertas conductas informáticas consideradas ilícitas con delitos previamente establecidos, queda al ánimo del juzgador la decisión final.

Analicemos tres de los casos, que, muy posiblemente lleguen a tribunales en relación con los virus, para que una vez expuestos podamos, a la luz del derecho, concretizar sobre el beneficio o perjuicio de los mismos.

Desde el punto de vista del programador, creador del virus, el mismo es sujeto de protección, más aún si se encuentra contenido en un programa aplicativo o en un sistema y, permanece inactivo en tanto no se realice una copia ilegal, puesto que la única copia que se autoriza al tenedor de un programa de computación es la de respaldo o backup (artículo 18 Ley Federal de Derechos de Autor). En consecuencia, cualquier otra copia con fines de lucro le valdrá una pena de 6 meses a 6 años de prisión y multa de 50 a 500 veces el salario mínimo (art. 135 de la misma Ley). Es de conocimiento general, que es prácticamente imposible el detectar a un trangresor del art. 135 citado, es en consecuencia, el virus, el medio eficaz para encontrar al culpable. En este orden de ideas, el copista que transgredió la ley, debe entonces, para liberarse del virus, contactar a la compañía distribuidora o bien al programador, para solicitar una vacuna o antídoto, previo registro como usuario autorizado, con todas las ventajas que se confieren como tal, por ejemplo el manual de operaciones, y la asistencia técnica. Hipotéticamente estas medidas diminuyen los casos de piratería autoral del software.

Segundo caso, supongamos que un virus creado con el solo propósito de protección, resulta ser mucho mas dañino de lo esperado, como le sucedió al Sr. Robert T. Morris Jr., y provoca cuantiosas pérdidas de información y programas ajenos; cierto es que, la propagación del virus derivó de una con-

ducta ilícita, pero también que, debido a una imprudencia del programador rogue, se ocasionaron cuantiosas pérdidas materiales, muy desproporcionadas a la simple copia del programa.

Tercer caso, en una actitud ciento por ciento dolosa, un programador rogue crea un virus «maligno» con el solo propósito de dañar los programas o sistemas de algún particular, sociedad o del público en general, podemos entonces afirmar que, se está atentando ya, contra la vida privada, violando el orden social, y en consecuencia incurriendo en una conducta ilícita.

Dice el Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, que los Derechos de Autor se consideran bienes muebles (art.758), siéndole por tanto, aplicables las disposiciones relativas a los mismos. Tomando en consideración lo anterior, considero que dentro del Código Penal del D.F., existe sólo un delito por el cual se puede inculpar a un programador rogue: EL DAÑO EN PROPIEDAD AJENA. Este delito se define en los siguientes términos:

> «Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena o de propia en perjuicio de tercero».

La penalidad establecida va desde los 2 a los 10 años de prisión, y multa de 100 a 500 veces el salario mínimo, segun la cuantía de lo dañado.

Estas podrían ser las sanciones a aplicar en el tercer caso hipotético visto anteriormente. Sin embargo, si la conducta del programador fue preterintencional, es decir, cuando se cause un resultado típico mayor al querido o aceptado, si aquel se produce por imprudencia (segundo caso), la pena se podrá reducir hasta una cuarta parte. Por otro lado, si el delito resultare ser totalmente imprudencial, esto es, se realiza un hecho típico incumpliendo un deber de cuidado, la pena sería de 2 días a 5 años de prisión.

Es sumamente difícil, desde el punto de vista jurídico-procesal, comprobar que alguien, a través de un virus, causó daño en propiedad de un tercero. Hace falta definitivamente, una regulación especializada que no se preste a excesos, y que regule especificamente estos delitos, para evitar confusiones e injusticia.

Si por cualquier motivo, estos virus llegaran a causar delitos superiores a la pérdida de información, me refiero especialmente a aquellos que afecten la vida o la integridad física de las personas, como estuvo a punto de ocurrir con el virus conocido como «SIDA», ¿qué decidirán los tribunales?. Relatare brevemente el caso:

Marzo 1989, diversos hospitales a lo largo de Europa, encuentran sus sistemas de registro y datos personales de pacientes, invadidos por un virus que deplegaba en pantalla un mensaje, informando que la computadora estaba infectada y que, para regresarla a la normalidad, debía mandarse un «donativo» a cierta dirección en Panamá; cómo este virus ponía en peligro la vida de pacientes, aunque los hospitales después se empeñaron en negarlo, di-

ciendo que sólo se trataba de un virus «benigno», se decidió que en vez de seguir un proceso legal de dudosos resultados, era más práctico, y menos riesgoso para ellos, contribuir con el donativo y recibir vía aérea la vacuna.

Un maestro de derecho penal, nos decía en sus clases, que la mente del delincuente, va un paso adelante de la del legislador, ya que este último regula y sanciona y el delincuente actúa para escapar de la aplicación de esa ley.

Los delitos informáticos son variados, desde los famosos «Hackers», ingreso a información confidencial, modificación de archivos, hasta el terrorismo informático. Las desastrosas consecuencias económicas o sociales no se ponen en duda, y de ello deriva la necesidad de un legislación penal actualizada que regule estas conductas claramente ilícitas.

Basta concluir que, independientemente de que la pena que la Ley Federal de Derechos de Autor mexicana señala para el caso de copia no autorizada de algún programa (piratería), es correcta, en la mayoría de los casos es letra muerta, por lo que para reducir los delitos negligentes o imprudenciales derivados de los virus, se debe primero aplicar de modo estricto dicha ley.

IV. DESDE EL PUNTO DE VISTA DEL DERECHO CIVIL

A la luz de lo ya analizado, puedo afirmar que, en relación con los efectos de los virus, en una demanda civil contra un programador rogue, para su procedencia, se requiere acreditar el derecho de autor violado o bien la propiedad de la información destruida por el virus.

Dos problemas se derivan de lo anterior, el primero se refiere al hecho de que la Ley Autoral consagra el Pricipio de Protección Automática, principio que trae como resultado que muchos programadores no registren sus creaciones y, el segundo, que la información utilizada por grandes empresas o personas a diario, NO ES OBJETO DE REGISTRO, en virtud de lo complicado que resultaría hacerlo, aunado a que dicha información puede cambiar de un momento a otro. De ello deriva que el demandar civilmente por daños y perjuicios, procederá sólo en el caso en que se logre comprobar la existencia y legal propiedad de la información y/o programas afectados, pruebas que en la práctica serán cubiertas por muy pocas personas, debido al desconocimiento de tales requisitos para acreditar la referida propiedad y, de que ninguna ley contempla disposiciones claras y objetivas en cuanto a pérdida de información, ya que únicamente se refiere al registro o no de los programas.

Un medio por el que civilmente, los usuarios podrían cubrirse del riesgo de perder su informacion, es la contratación de seguros, donde, en caso de siniestro, la empresa aseguradora pagaría los daños, subrogándose a su vez en nuestro derecho de demandar al creador del virus. En Estados Unidos, se ha comenzado ya a otorgar pólizas de este tipo, con muchas limitaciones y lagunas, pero cobertura al fin y al cabo.

V. INFLUENCIA INTERNACIONAL

Es conveniente antes de cerrar este estudio, hablar acerca de la tendencia que a la fecha esta tomándose en Europa, a raíz de la Propuesta de Directiva de Programas de Ordenador de la Comunidad Económica Europea, ya que tendrá seguramente, gran influencia futura en los criterios de los juzgadores en todo el mundo. Quiero referirme especialmente al articulo 7o. de dicha propuesta, que a la letra menciona:

«...Art. 7. Medidas especiales de proteccion:

1. Sin perjuicio de las disposiciones de los arts. 4, 5 y 6, los Estados miembros, de conformidad con sus legislaciones nacionales, deberán adoptar medidas adecuads contra las personas que cometan cualquiera de los actos mencionados en las letras siguientes:

a...

b...

c. La puesta en circulación o tenencia con fines comerciales de cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador.»

2...

3. Los Estados miembros podrán ordenar la confiscación de los medios a que hace referencia la letra c del apartado 1.

En una primera lectura, se entiende que las vacunas son un medio de eliminar dispositivos técnicos de protección, el hecho es que, si queremos copiar un programa que sabemos está protegido por un virus, estamos cometiendo el delito de reproducción no autorizada y, en consecuencia, la utilización de una vacuna esta prohibida, aún y cuando la finalidad con la que se utilice NO SEA COMERCIAL. Ahora bien, suponiendo que el virus es ajeno a nosotros, y que se transmitió a través de una red o de comunicación vía satélite, y se usa la vacuna para desinfectar nuestros programas infectados, materialmente no estaríamos sujetos a la aplicación del punto uno del artículo citado, pero si la autoridad requiere que se entreguen las vacunas, como se contempla en el punto 3, deberá hacerse y, en consecuencia, ¿cómo van a cubrirse los usuarios?.

No se toma en cuenta tampoco, que hay casos en los que son los mismos programadores quienes incluyen en sus creaciones los virus, a efecto de poder después transmitir las vacunas, creadas también por ellos, mediante previa «donación», excluyéndose así, del ámbito de aplicación de dicha norma, puesto que repito, no tendría una finalidad comercial ya que que no se está vendiendo, sino solicitando opcionalmente una ayuda altruista para continuar con sus investigaciones.

El documento que se analiza, no menciona nada al respecto de la pérdida de información derivada de la programación rogue, ni de hasta qué grado los dispositivos técnicos de protección son o no lícitos.

A mi punto de vista deberían de especificarse los dispositivos a los que se refiere, puesto que si los mismos se usan para proteger información confidencial, estoy de acuerdo en la supresión de los medios que los eliminen, por otro lado, si se contempla a los virus, este precepto no es de tan lógica aplicación.

Evidentemente, las vacunas no deben ser estrictamente prohibidas, como tampoco lo deben ser los virus, pero es de tener siempre en cuenta que somos una comunidad, y como tal, nuestro derecho llega hasta donde empieza el derecho ajeno.

VI. CONSIDERACIONES FINALES.

Se ha repetido hasta el cansancio que la única manera de acabar con los virus es reduciendo el riesgo de contagio, evitar introducir paquetes de dudoso origen, realizar continuamente revisiones de los discos, reportar oportunamente cualquier irregularidad, etc. Es cierto que estas acciones pueden minimizar el peligro, pero no lo erradican. El problema entonces, se centra en determinar si los virus y las vacunas deben ser reguladas o prohibidas.

Desde el punto de vista ético, quizá los virus no sean el medio idóneo para buscar la protección de un programa, pues al activarse es posible que cause daño tanto en la parte material, como en la inmaterial de un sistema de cómputo. Por otro lado, si un virus está diseñado para evitar la reproducción ilícita de un programa, el aplicar una vacuna para suprimirlo implica ya en sí, una conducta ilícita. La contraposicion de ambas ideas es evidente.

Si toda la gente se guiara por normas éticas tan sencillas como el respeto al derecho de terceros, las leyes no tendrían razón de ser, sin embargo, como humanos que somos, estamos repletos de pasiones y errores, unos más que otros, pero al fin y al cabo somos todos iguales.

Como manifesté antes, cada persona tiene derecho a proteger lo que es suyo, siempre y cuando no se violen los derechos ajenos. Hablando de virus, no se debe ser tan duro en contra de quienes buscan una protección real para sus creaciones, protección que obviamente no ha conseguido otorgar el Derecho de Autor. Si se quiere atajar un mal, se debe empezar por sus raíces, y después por sus ramas, de tal manera resulta indispensable, no sólo combatir la piratería, sino comenzar por proteger debidamente el software, regulándolo de manera global. Por esto último, me refiero a todos los aspectos del derecho, desde cómo otorgar protección hasta la especificación de las penas provenientes de conductas que puedan ser consideradas como ilícitas, en pocas palabras, una codificación informática que pueda sentar las pautas y crite-

rios base para evitar el robo, copiado no autorizado, pérdida de información propiedad de terceros, etc.

No se pueden atacar los virus como si fueran el némesis de todo programador, tomando en cuenta que fuimos nosotros mismos quienes provocamos su generación, tampoco es conveniente prohibir que se inventen medios para defendernos y mucho menos venderlos, puesto que su creación misma ya implicó cierto esfuerzo intelectual, que por justicia social debe ser remunerado; pero seamos realistas, hay un gran porcentaje de virus informáticos que se crean con el solo fin de perturbar la paz, por demostrar las habilidades de un programador, o por simple venganza, son esos virus los que deben de ser penados; el dolo, la mala fe, el ánimus de la creación es la que marca la diferencia entre defensa y ataque, porque estoy seguro que si elaboramos una base firme de protección del software, una gran parte de los virus, sobre todo aquéllos que por negligencia o preterintención se han propagado desorbitadamente, desaparecerían.

El Seguro de Responsabilidad Civil Profesional de los Informáticos

PAUL VAN HOUTTE
Centro de Investigación de Informática y Derecho. (CRID).
(BELGICA)

INTRODUCCION: DEFINICION DE LA POLIZA DE SEGUROS QUE EL PRESTADOR DE SERVICIOS INFORMATICOS TIENE QUE TOMAR PARA CUBRIR SU ACTIVIDAD PROFESIONAL

El seguro de la responsabilidad civil en general, que la empresa toma por correr riesgos en el ejercicio de su explotación, se llama seguro de la responsabilidad civil explotación. Estos riesgos son corridos tanto por las empresas industriales como, en menor medida, por los prestadores de servicios.

Para cubrir los riesgos corridos en el ejercicio de su actividad profesional específica –y no sólo los riesgos corridos por tener la empresa funcionando– se necesita otro seguro suplementario.

Dichas pólizas son específicas para cada tipo de actividad.

La póliza responsabilidad civil profesional (en sentido estricto) cubre la actividad intelectual del prestador de servicios.

He aquí unos ejemplos de prestadores de servicios:

1) Los profesionales liberales (médicos, ...) que ejercen una actividad civil.

2) Las profesiones comerciales de servicio jurídico (abogado), contable (experto contable) y financiero (los banqueros).

3) Los prestadores de servicios informáticos son otra categoría.

La responsabilidad cubierta es la responsabilidad tanto contractual como extra-contractual, en la cual el prestador ha incurrido por haber causado daños por la venta de programas informáticos estandarizados y/o haber prestado servicios y consejos, en relación con sistemas de tratamiento de la información.

Estos daños resultarían de la culpa profesional y/o de la falta de obediencia a las reglas del arte.

En estas pólizas se pueden encontrar dos particularidades respecto de las otras pólizas de responsabilidad civil profesional:

1) El asegurador no sólo tiene la obligación de indemnizar los daños sufridos por la persona acreedora pero además tiene un papel en el tratamiento del daño. Para acabar de manera eficaz con un daño, hay que construir un ambiente de conciliación, en el cual el asegurador actúe como intermediario. Para la continuidad de la empresa deudora, este papel es muy importante.

Este papel es todavía más claro en las pólizas «garantía de éxito de un proyecto informático», concluídas directamente por el cliente de un prestador de servicios informáticos.

Por su naturaleza jurídica, el seguro de responsabilidad ya no es –en estos casos– una garantía de la deuda del profesional, sino que se convierte en una garantía de crédito de la indemnización de las víctimas.

La subrogación posible en favor del asegurador ya no se hace en la persona del profesional, sino en la persona del cliente. En efecto, el asegurador conserva un recurso contra el responsable de la obra.

Por esta razón, el asegurador se encargará activamente del proyecto. Antes de firmar la póliza el asegurador ejerce un control sobre las posibilidades de éxito del proyecto. Luego, una vez firmada la póliza, seguirá la realización del proyecto para, por ejemplo, encontrar rápidamente los siniestros.

2) Hay también una segunda particularidad.

Desde la integración de la directiva europea 85/374 del 25 de julio de 1985 sobre la responsabilidad derivada de los productos, es importante preveer en la póliza de responsabilidad civil profesional la cobertura de dichos riesgos.

1. ¿Qué cubre la garantía? Descripción de las actividades y de los riesgos acontecimiento (hechos generadores de los daños, para los cuales la póliza prevé cobertura).

Los límites del seguro responsabilidad civil profesional son dados por la definición de la profesión, la calificación del profesional y por la exclusión de los actos prohibidos por la profesión.

1.1. Definición de la profesión

Las actividades de las empresas industriales y de servicio en informátilca son la fabricación y el suministro de:

– Material (hardware)
– Programas informáticos estandarizados (software)
– Prestaciones de servicio

Las dos últimas actividades son cubiertas por la póliza, como lo hemos visto más arriba.

La prestación de servicios incluye:

– Desarrollar los sistemas y asesorar sobre ellos.
– Escribir y validar programas.
– Suministrar programas, aplicarlos a los ordenadores y formar el personal usuario.

Los riesgos referidos son los de concepción, realización y funcionamiento de los programas específicos o estandarizados.

Estos son la consecuencia clara de la definición de la profesión pero muchas veces la póliza describe los riesgos cubiertos y/o los riesgos excluídos.

En Bélgica, el sistema es lo siguiente: Las pólizas cubren todos los riesgos salvo los determinados en una larga lista de exclusiones.

1.2. Las exclusiones de los actos prohibidos por la profesión.

La calificación jurídica de estas exclusiones puede ser doble:

1) Primero, hay las llamadas exclusiones-frontera: el asegurador marca las líneas de la profesión para tener una competencia delimitada de la garantía.

2) Segundo, las llamadas exclusiones-hueco, sacan de entre las líneas de la profesión un acontecimiento para excluirlo.

Los ordenamientos jurídicos europeos desconfían en principio de esta técnica de exclusiones.

Las primeras son por esencia más largas, las segundas deben ser claras y estrechamente definidas, pues si no podrían ser anuladas por los tribunales.

En Bélgica, por ejemplo, el tribunal juzgará –previa petición del interesado– si la exclusión puede ser interpretada como una exclusión de culpa

grave. El artículo 8*2 de la ley del 25/06/1992 sobre el contrato de seguro dice: «El asegurador puede exonerarse de sus obligaciones, en los casos de culpa grave determinados expresa y limitativamente en el contrato».

1.3. La calificación del profesional.

Para los prestadores de servicios informáticos no existe una ley que regule la profesión, por ejemplo, exigiendo un título para practicar dicha actividad. Sin embargo, las empresas pueden imponerse a sí mismas algunas normas. Existen dos sistemas de normas:

1.3.1. *Un sistema ya establecido,* según el cual una empresa obtiene un certificado de conformidad para sus productos.

1.3.2. *Un nuevo sistema: asegurar (en inglés:«assurance»= insurance) la gestión de la calidad.*

Se trata de una práctica más reciente que consiste en examinar la conformidad del «sistema de calidad» del prestador de servicios a las normas ISO-9000 (y para los prestadores de servicios informáticos a las normas ISO 9001). Para ello se realiza un conjunto de pruebas objetivas de las precauciones, tomadas durante el ciclo de producción, para obtener un producto final con un nivel de calidad determinado.

Por lo tanto, dichos test no están efectuados en un producto específico, sino a todo el ciclo de producción, ya sea durante la fase de concepción, producción, reproducción o distribución del producto.

Los test y controles conciernen pues los individuos, materiales, instrumentos y métodos que permiten la existencia del producto y no del producto en sí mismo.

La certificación del sistema de control de calidad del prestador puede así ofrecer al consumidor la certeza, no tanto de que el producto sea de calidad sino que la organización proceso de producción sea correcta y controlada. El cliente tiene pues la certeza que el productor sea capaz de producir, por ejemplo, un software de manera conforme con las normas establecidas para tal producto (normas ISO-9001)

La existencia de las normas de gestión de la calidad es interesante para la empresa y también para el asegurador.

En la póliza responsabilidad civil de automóviles, el asegurador belga exige a cada tomador de seguro que su vehículo haya superado un control técnico.

Así también, el asegurador podría exigir que el prestador de servicios, haya obtenido el certificado de conformidad a las normas ISO-9001. Es un método para seleccionar los riesgos y prevenir los siniestros.

Supongamos que el contrato de seguro exija al asegurado un certificado. ¿Qué pasaría si el prestador de servicios utiliza la marca de conformidad en

sus productos sin respetar las condiciones de uso, tal y como están previstas en el reglamento específico?

Está claro que los siniestros en este caso no estarían cubiertos por el asegurado. Pero, según la redacción y la interpretación del contrato, la sanción puede ser distinta: hay que analizar la voluntad de las partes contratantes, sobre todo la del asegurado. Para excluir un riesgo, el asegurador la menciona explícitamente; por lo contrario, los casos de agravación de riesgos pueden ser cubiertos.

2. Responsabilidades cubiertas por la póliza responsabilidad civil profesional (en sentido amplio): la responsabilidad civil profesional (en sentido estricto) y la responsabilidad derivada de los productos.

Hemos de hacer una primera distinción entre la responsabilidad del prestatario para con su cliente (responsabilidad interna o directa) y la responsabilidad para con una tercera persona o un cliente de una tercera persona (responsabilidad indirecta o externa).

El primer tipo sería más bien una responsabilidad contractual, el segundo tipo una responsabilidad extracontractual.

La segunda distinción es entre la responsabilidad subjetiva y objetiva.

El seguro de la responsabilidad civil profesional cubre los daños que resultan de «errores», «negligencias» o «fallos cometidos» en el ejercicio de la profesión. Esta terminología garantiza pues una responsabilidad subjetiva basada en la culpa probada o presumida, extracontractual o contractual (en el caso de una «obligación de medios», muchas veces para el suministro de programas informáticos específicos para el cliente).

Sin embargo hoy en día la responsabilidad profesional exigida por la ley y la jurisprudencia es cada vez más una responsabilidad objetiva. Pues hay que esperar que la redacción de las pólizas abandone el concepto tradicional de culpa para incluir toda responsabilidad exigida por el ordenamiento jurídico existente. Existen ya dos casos de responsabilidad objetiva:

– a nivel contractual en las «obligaciones de resultado» (suministro de programas informáticos estandarizados).

– desde la integración de la directiva europea 85/374 del 25 de julio de 1985 en los ordenamientos jurídicos nacionales y en el caso que la directiva se aplique a los programas informáticos, existe un sistema de responsabilidad objetiva fundada en la falta de seguridad del producto. Los aseguradores temerán probablemente en cubrir la responsabilidad objetiva. Pero, ¿no es la actividad de las compañías de seguro de cubrir casualidades e incertidumbres?

La actividad aseguradora tiene que adaptarse a las exigencias modernas de responsabilidad objetiva, si no se multiplicarán los fondos de garantía que le quitarán toda preocupación... cogiendo su sitio.

3. Descripción del riesgo objeto de la garantía.

La garantía del riesgo profesional tiene que precisar las víctimas, el responsable, los daños, la fecha del sinientro, y su montante.

Solo hablaremos aquí un rato de los daños pues es la particularidad del seguro de la responsabilidad civil profesional respecto de la póliza responsabilidad civil explotación, que cubre sólamente las lesiones corporales y los daños materiales.

En la póliza responsabilidad civil profesional, los daños considerados son más bien las pérdidas pecuniarias, que sean o no consecuencia de los daños materiales.

BIBLIOGRAFIA

Legislación:

Ley Belga del 25/06/1992 sobre el Contrato del Seguro Terrestre.

Directiva europea 85/374 del 25/07/1985 sobre la responsabilidad derivada de productos.

Doctrina:

COUSY, H., «Verzekeringsrecht», 1990.

KASPERSEN, H.W.K., OSKAMP, A., «Amongts Friends in Computers and Law», Kluwer, Deventer, 1990.

LUCAS, A., «Le droit de l'informatique», Paris, P.U.F., 1987.

KEUSTERMANS, J., «Computerverzekering», Makelaarspraktijk (praktijkboecK verzekeringsbemiddeling), 1989.

MEERSMAN, J., VAN KEER, A., «Les contrats informatiques: réflexions sur 10 ans de jurisprudence belge et française», J.T., 1982, p. 1-9, p. 17-26.

ULLMAN, P., «Assurances de l'informatique», in Les Assurances de l'entreprise, 1988.

VANDENBERGHE, G., «Partijenaansprakelijkheid bij softwarecontracten», 1984.

X., «Informaticacontracten», Kluwer, Antwerpen, Deventer, 1992.

X., «Informaticarecht: de actuale stand van zaken», 1990.

MESA N.º 5.–DELITOS INFORMATICOS

«Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial»

M.ª CARMEN ALASTUEY DOBÓN

Area de Derecho Penal. Facultad de Derecho de la Universidad de Zaragoza

(ESPAÑA)

1. NOCION

Intentar determinar qué se entiende por «criminalidad informática» o más concretamente por «delito informático» no es tarea fácil, sobre todo si se tiene en cuenta que ambas expresiones no han sido aceptadas por la doctrina acríticamente. El término «delito informático» resulta especialmente problemático y ello a pesar de que es utilizado por la mayoría de los autores españoles dada su plasticidad [1]. Se dice, en primer lugar, que no puede hablarse de «delito» para aludir a un comportamiento no tipificado como tal en el C.P.[2] CAMACHO LOSA advierte la falta de tecnicismo del término pero, a pesar de ello, lo usa deliberadamente [3]. Sin embargo, a mi juicio, la principal objeción a dicho término la constituye el hecho de que, como dice ROMEO, no hay un «delito informático» sino una pluralidad de ellos con una única nota común: su vinculación con el ordenador [4]. Por todo esto, quizá resulte más adecuado hablar de «delincuencia o criminalidad informática» como ca-

(1) ROMEO CASABONA, C. «Poder informático y seguridad jurídica». Madrid, 1987 p.41
(2) GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». Madrid, 1991 p.51
(3) CAMACHO LOSA, L. «El delito informático». Madrid, 1987, p. 26
(4) ROMEO CASABONA, C. «Poder informático». cit. p.41

tegoría exclusivamente criminológica [5] en espera de una reforma penal que aclare la situación.

Pero, como apuntaba al principio, la definición del fenómeno no es tampoco unánime. Mencionaré sólo algunas de las definiciones citadas por los autores. TIEDEMANN considera que con la expresión «criminalidad mediante computadoras», se alude a «todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamenteo de datos» [6]. ROMEO se refiere a la definición propuesta por el Departamento de Justicia Norteamericano, según la cual «Delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución» [7]. RUIZ VADILLO recoge la definición que adopta el mercado de la OCDE: «Abuso informático es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos» [8], [9].

Por otra parte, surgen nuevos problemas al intentar esclarecer a qué forma de criminalidad se hace referencia cuando se habla de «delincuencia informática». La doctrina, casi unánimemente, la considera inscribible en la criminalidad de «cuello blanco» [10]. Otros la incluyen en la delincuencia económica. RUIZ VADILLO, por ejemplo, cita la Recomendación número R (81) 12 del Consejo de Europa en la que la criminalidad informática es considerada como una forma de la delincuencia económica [11]. El mismo RUIZ VADILLO cree que «toda la fenomenología de la delincuencia económica es aplicable mutatis mutandis a la materia informática» [12]. TIEDEMANN inscribe la «criminalidad mediante computación» entre las formas de criminalidad económica «neutrales», es decir, entre las que surgen en cualquier sistema económico con independencia de la naturaleza del mismo. Por tanto, también TIEDEMANN incluye la «criminalidad por computadoras» entre la criminalidad económica, aludiendo a la parte de aquélla que perjudica los intereses patrimoniales y no a la que perjudica la intimidad [13].

Llegados a este punto, creo que no resulta reiterativo recordar la definición que de delincuencia de «cuello blanco», diera en su día SUTHERLAND:

---

[5] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p.62

[6] TIEDEMANN, K. «Poder económico y delito». Barcelona, 1985. p.122

[7] ROMEO CASABONA, C. «Poder informático». cit. p.42

[8] RUIZ VADILLO, E. «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica». Poder Judicial. Número especial IX, 1988. pp. 58 y 59

[9] Otros intentos de definición pueden encontrarse en GUTIERREZ FRANCES, M.L. «Fraude informático y estafa». cit. pp. 53 a 58 y en CAMACHO LOSA, L. «El delito informático». cit. pp. 25 y ss.

[10] En este sentido, GUTIERREZ FRANCES, M.L. «Fraude informático y estafa» cit. p.73

[11] RUIZ VADILLO, E. «Tratamiento de la delincuencia informática...» cit. p. 56

[12] RUIZ VADILLO, E. «Tratamiento de la delincuencia informática...» cit. p. 63.

[13] TIEDEMANN, K. «La criminalidad económica como objeto de investigación» Cuadernos de Política Criminal. Número 19, 1983. p.173

«violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional"[14]. Si, además, tenemos en cuenta la definición que se adopta de delincuencia económica desde el punto de vista criminológico, entendiendo por ella la «relativa a las infracciones lesivas del orden económico cometidas por personas de alto nivel socio-económico en el desarrollo de su actividad profesional» [15], deberemos afirmar, que los autores que inscriben la criminalidad informática entre la delincuencia económica, están de acuerdo en inscribirla también entre la delincuencia de «cuello blanco»; y ello aunque consideremos con BAJO que la delincuencia económica es, en puridad, una especie de la de «cuello blanco» y que por eso no debe identificarse aquélla con ésta sin establecer el matiz correspondiente [16]. Pues bien, si analizamos ambas definiciones, encontramos en ellas un elemento común que nos interesa aquí especialmente: el hecho de que el autor de la infracción posea un «alto nivel socio-económico», elemento del que no puede prescindirse en estos conceptos criminológicos porque, como indica BAJO, este elemento evidencia que los efectos de la infracción son más lesivos, por su cuantía, por el número de personas afectadas y porque éstas suelen pertenecer a clases modestas [17]. Ambas definiciones hacen referencia, en consecuencia, a un determinado tipo de autor. Por ello, desde este punto de vista, creo que la delincuencia informática no es subsumible en ninguno de los dos tipos de delincuencia citados, sino que debe constituir una categoría criminológica aparte [18], puesto que en las investigaciones empíricas llevadas a cabo en Estados Unidos, principalmente, se constata que el autor sólo en ocasiones pertenece a las altas capas de la sociedad. Y esto último es reconocido por la doctrina española. Así, ROMEO pone de relieve que los autores suelen ser primarios u ocasionales y que generalmente se trata de empleados de las empresas afectadas [19]. GUTIERREZ se refiere a la caracterización casi mítica que se ha venido efectuando del delincuente informático como adolescente de posición social media (con lo que, por cierto, tampoco entraría en la categoría de delincuente «cuello blanco») y cree que se trata, más bien, de empleados de empresas con acceso a su sistema informático, o incluso chavales jugando con el ordenador o amas de casa [20]. RUIZ VADILLO se muestra reticente a identificar a este tipo de autor con el delincuente propio de la criminalidad de los negocios y caracterizado por las notas que encontró Mer-

---

[14] Véase por todos GARCIA-PABLOS DE MOLINA, A. «Derecho Penal y criminalidad financiera» En su libro «Estudios Penales». Madrid, 1984. p. 288

[15] Definición que «no es más que la adaptación a la delincuencia específicamente económica de la definición que Sutherland en 1939 refirió a la delincuencia de «cuello blanco». BAJO FERNANDEZ, M. «Manual de Derecho Penal. Parte Especial». Madrid, 1987. p. 399

[16] BAJO FERNÁNDEZ, M. «Derecho Penal Económico». Madrid, 1978. p. 49

[17] BAJO FERNÁNDEZ, M. «Derecho Penal Económico». cit. p. 49

[18] En el mismo sentido, RUIZ VADILLO, E. «Tratamiento de la delincuencia informática...» cit. p. 64, siguiendo a TIEDEMANN.

[19] ROMEO CASABONA, C. «Poder informático...». cit. p. 36

[20] GUTIÉRREZ FRANCÉS, M.L. «Fraude informático y estafa». cit. pp. 74 y 79

gen en él, notas con las que elaboró su famoso psicograma [21],[22]. CAMACHO LOSA también cree que los autores de estas infracciones son empleados de confianza de las empresas afectadas, en la mayoría de los casos, que tienen acceso al sistema informático y conocen sus debilidades [23]. Por último, también TIEDEMANN sostiene que los autores suelen ser principiantes o casuales y no poseen una inteligencia superior a la media [24]. No creo que los empleados de las empresas afectadas puedan considerarse personas pertenecientes a las altas capas sociales, en el sentido en que es utilizado el término en el concepto de delincuencia de «cuello blanco». Creo, además, que este concepto debería ser revisado. No todo acto lesivo del orden económico es subsumible en la categoría de delincuencia de «cuello blanco», tendencia muy generalizada hoy en día. Debe atenderse, en cada caso concreto, al tipo de autor [25].

A modo de conclusión: Se ha comprobado que, en la mayoría de las ocasiones, el «delincuente informático» no posee un alto nivel socio-económico y como esta característica es esencial en el concepto de delincuencia de «cuello blanco», creo que la delincuencia informática no puede identificarse, desde un punto de vista criminológico con la reiteradamente citada delincuencia de «cuello blanco».

2. CIFRA NEGRA Y SUS CAUSAS

Es innegable que existe criminalidad informática en España, puesto que las nuevas tecnologías se han implantado también en nuestro país y cuando se generaliza el uso de nuevas tecnologías, aparecen inevitablemente nuevas formas de criminalidad. Sin embargo, resulta imposible calcular la incidencia de dicha criminalidad dada la inexistencia de investigaciones empíricas al respecto, y en España, sólo unos pocos casos han salido a la luz [26]. CAMACHO LOSA se refiere al «muro de silencio que rodea todo lo relacionado con el delito informático» y menciona como «honrosa excepción» al Banco Popular Español que «acostumbra a incluir en sus memorias algunos de estos casos,

---

[21] RUIZ VADILLO. «Tratamiento de la delincuencia informática...» cit.p.63

[22] Mergen intentó determinar las características de la personalidad del delincuente de «cuello blanco» y encontró en ellas las siguientes notas: Materialismo, egocentrismo y narcisismo, dinamismo y audacia, inteligencia, peligrosidad, hipocresía, neurosis y conciencia de culpabilidad. Esta descripción fue muy criticada, pues Mergen no probó como debiera la realidad de sus análisis. Más extensamente en BAJO FERNÁNDEZ, M. «Derecho Penal Económico» cit. pp. 53 y ss.

[23] CAMACHO LOSA, L. «El delito informático». cit. p. 84

[24] TIEDEMANN, K. «Poder económico y delito». cit. p. 126

[25] No debe olvidarse el momento histórico en que surgió el concepto de «delincuente de cuello blanco» ni tampoco los prejuicios neopositivistas de que dicho concepto adolece. Al igual que en la ya superada criminología positivista, se consagra un tipo de autor que, aunque nuevo merece críticas similares. Ver al respecto, GARCIA-PABLOS DE MOLINA, A. «Derecho Penal y criminalidad financiera...» En Estudios Penales. cit. pp. 228 y ss.

[26] ROMEO CASABONA, C. «Poder informático». cit. p. 37

comentando las circunstancias que rodearon el hecho y las consecuencias del mismo» [27]. Pero las investigaciones que se han llevado a cabo en Estados Unidos ponen de relieve que la «zona oscura» más elevada se da en los «delitos perpetrados en conexión con los medios informáticos» [28]. GUTIERREZ, aludiendo a la elevada cifra negra en esta criminalidad, señala que, incluso en los países en que se han detectado un mayor número de casos, éstos sólo representan «la punta del iceberg» [29]. TIEDEMANN pone de manifiesto la imposibilidad de realizar un cálculo siquiera aproximado de la cifra negra en este ámbito y, refiriéndose al caso alemán, señala que, en la mayoría de los procesos penales, el descubrimiento de los hechos se produjo por pura casualidad [30].

Se apuntan varias CAUSAS DE ESTA ELEVADA CIFRA NEGRA EN EL AMBITO DE LA CRIMINALIDAD INFORMATICA.

Por un lado, no existen todavía medios adecuados de detección y control de los hechos. Un sistema complejo de control no resultaría beneficioso a las empresas que precisamente buscaron rentabilidad económica y ahorro de tiempo con la instalación de equipos informáticos [31].

Por otra parte, la víctima desconoce el hecho la mayoría de las veces o, aún conociéndolo y sospechando fundadamente quién lo cometió, tiene dificultades para probar ambas cosas (tanto la perpetración del hecho como su autor). Ciertamente, descubrir el hecho no resulta fácil; las propias características del mismo lo impiden: los medios complejos de comisión del hecho que son conocidos exclusivamente por especialistas en sistemas informáticos, la facilidad del autor de borrar toda huella que pueda inculparle, la separación temporal entre lugar de comisión del hecho y de producción de los efectos, etc. Con todo esto, lo cierto es que estos «delitos» suelen descubrirse por casualidad [32]. A las dificultades de descubrimiento se suman las de prueba en el proceso de estos hechos por las mismas causas señaladas más arriba [33].

En otras muchas ocasiones, la víctima no denuncia los hechos, pues teme que, reconocer que ha sido objeto de uno o varios de estos comporta-

---

[27] CAMACHO LOSA, L. «El delito informático». cit. p. 69

[28] ROMEO CASABONA, C. «Poder informático». cit. p. 36. Advierte ROMEO que cuantificar la zona oscura resulta difícil puesto que los estudios criminológicos al respecto no son suficientemente rigurosos.

[29] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p. 72

[30] TIEDEMANN, K. «Poder económico y delito». cit. p. 123

[31] ROMEO CASABONA, C. «Poder informático». cit. p. 38. También CAMACHO LOSA, L. «El delito informático» cit. p. 70, hace referencia a la casi total ausencia de medidas de seguridad en las instalaciones.

[32] Véase, por todos, CAMACHO LOSA, L. «El delito informático», cit. p. 70, apunta que, probablemente los casos conocidos hubieran quedado en el anonimato de no ser por la casualidad.

[33] GUTIÉRREZ FRANCÉS, M. L «Fraude informático y estafa» cit. pp. 80 y 81.

mientos, pueda incidir negativamente en el buen nombre de la empresa, con la natural desconfianza hacia la misma por parte de los clientes de la entidad que surgiría al comprobar que carecía de las medidas de seguridad adecuadas. Además, a las empresas afectadas les resulta más rentable una solución privada del problema, pues, como dice TIEDEMANN, consideran que si se impusiera una pena privativa de libertad al autor del hecho, dejaría de trabajar y de percibir una remuneración, con lo que disminuiría considerablemente la posibilidad de aquél de reparar el daño causado [34]. Por otro lado, la víctima (en general y no sólo la de delincuencia informática), desconfía de que los tribunales puedan solucionar su problema [35].

CAMACHO LOSA añade entre las causas que influyen en el hecho de que los autores de un delito informático no sean denunciados, la falta de una legislación adecuada al respecto [36].

3. LA VICTIMA

Como puede deducirse de las páginas anteriores y como demuestra la experiencia extranjera y los pocos casos que se han dado a conocer en España, las víctimas del ilícito informático son, casi sin excepción, personas jurídicas. Parece ser que, por regla general, se trata de bancos o compañías de seguros o empresas del sector pero, como advierte ROMEO, también las empresas públicas son víctimas de estos ilícitos y pone como ejemplo de estos últimos casos las diversas actividades de los servicios postales o de la Seguridad Social [37].

También mediante la observación de los casos conocidos, GUTIERREZ llega a la conclusión de que suele tratarse de «personas jurídicas con un potencial económico muy elevado, y que, por lo general, no gozan de muy buena prensa entre el ciudadano medio». Además, y enlazando con el apartado anterior, las víctimas suelen actuar como «colaboradoras» del hecho: rara vez denuncian las conductas ilícitas, en pocas empresas se protegen los sistemas informáticos con medidas de seguridad y controles adecuados, las empresas cometen a veces errores que propician la comisión del hecho al autor potencial.... [38]

4. LOS HECHOS

Las características de los hechos, aunque fácilmente deducibles de lo ya examinado hasta ahora, pueden resumirse de este modo:

---

[34] TIEDEMANN, K. «Poder económico y delito». cit. 123. Ver también ROMEO CASABONA, C. «Poder informático». cit. p. 39 y RUIZ VADILLO, E. «Tratamiento de la delincuencia informática... cit. p. 57

[35] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p.72

[36] CAMACHO LOSA, L. «El delito informático». cit. p. 70

[37] ROMEO CASABONA. C. «Poder informático». cit. p. 39

[38] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa» cit. p. 76

a) Estos hechos procuran a sus autores unas elevadas ganancias. El perjuicio económico que producen es muy superior al de cualquier otro tipo de conducta ilícita, también al causado por la delincuencia económica. Se da, además, el anonimato del perjuicio producido [39].

b) Por regla general, estas conductas no se llevan a cabo con un único acto sino mediante una serie continuada de ellos. Es decir, esta forma de delincuencia tiene un EFECTO CONTINUADO. Si en la primera intromisión en el sistema informático se logra tener éxito, el autor suele continuar con la comisión de actos ilícitos [40].

c) Entre el hecho ilícito y los efectos del mismo existe una separación temporal [41].

d) Una vez cometido el ilícito, el autor consigue borrar todas las huellas, sin dejar rastro perceptible, lo que hace que disminuya considerablemente el riesgo de ser descubierto [42].

e) Los autores del «delito» no suelen ser personas con una inteligencia superior a la media que poseen conocimientos cualificados en el campo de la informática y que por ello llevan a cabo manipulaciones sofisticadas en los sistemas informáticos, sino más bien personas con un coeficiente intelectual medio, que tienen la «oportunidad» de realizar el hecho y la aprovechan [43]. En este sentido, creo que el móvil del autor es, en la mayor parte de los casos, «sencillamente», el ánimo de lucro, aunque pueda haber otros móviles complementarios [44].

5. POSIBLES SOLUCIONES

Para luchar contra la delincuencia informática, las medidas preventivas juegan un papel primordial. Las empresas se muestran reacias a proteger su

---

[39] ROMEO CASABONA, C. «Poder informático». cit. p.35, GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. pp. 78 y 79. CAMACHO LOSA, L. «El delito informático». cit. pp. 69 y ss, GONZÁLEZ RUS, J. J. «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos» Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12. Monográfico sobre informática y derecho, 1986. TIEDEMANN, K. «Poder económico y delito». cit, pp. 123 y ss y otros.

[40] Véase TIEDEMANN. K. «Poder económico y delito» cit. p. 123 y en el mismo sentido GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p. 79

[41] Véase nota anterior.

[42] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa» cit. p. 79 y ROMEO CASABONA, C. «Poder informático» cit. p. 35

[43] En este sentido CAMACHO LOSA. L «El delito informático» cit. p. 83 asegura que el perfil de estas personas en general no es el de un delincuente, sino que «se trata de personas que podríamos encuadrar en lo que coloquialmente denominamos gente del montón que por azar, por diversión, o por investigación técnica han descubierto ciertas debilidades en el sistema que les pone en situación de poder aprovecharse de dicha circunstancia, y coyunturalmente se encuentran en una situación en la que sin ser desesperada no les vendría mal un puñado de dinero extra».

[44] Ver GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa» cit. p. 75 y 76. También GONZÁLEZ RUS, J.J. «Aproximación al tratamiento penal» cit. p. 111.

sistema informático de manipulaciones ilícitas mediante la adopción de rigurosas medidas de seguridad y controles pues supondría una pérdida considerable de tiempo y dinero que, creen los directivos de algunas entidades, superaría quizá el perjuicio económico causado por un «delito» informático esporádico y aislado. Es verdad, como CAMACHO LOSA deja patente [45], que la adopción de sistemas de seguridad de esta envergadura, supone un esfuerzo de trabajo, económico, el nacimiento de nuevas responsabilidades, la necesidad constante de renovación de dicho sistema. Pero, como el mismo autor señala, estos controles permitirían detectar la situación anormal y frecuentemente minimizar sus consecuencias; y en todo caso, posibilitarían descubrir al autor y probar su culpa ante los tribunales [46].

Pero sin acudir a estas sofisticadas medidas, existen otras más fáciles de poner en práctica por parte de las empresas y con ellas es posible obtener resultados satisfactorios. Entre estas medidas se cuentan: la separación física del departamento de informática del resto de las instalaciones de la empresa; la separación de funciones, de modo que no cualquier empleado pueda acceder a los ordenadores; el cambio frecuente de los códigos de acceso; la identificación de los empleados autorizados para el uso del ordenador cada vez que vayan a manejarlos; la posibilidad de que las terminales se desconecten automáticamente tras cierto tiempo de inactividad; la realización de auditorías internas y externas con expertos informáticos e incluso el concierto de seguros para cubrir los riesgos de los perjuicios derivados de un posible ilícito informático [47].

La delincuencia informática patrimonial puede prevenirse más fácilmente que la delincuencia clásica contra el patrimonio. Pero cuando las medidas preventivas que se adopten no resulten suficientes para evitar la comisión del hecho (o bien no se ha adoptado ninguna) y el ilícito se haya cometido efectivamente, deberán determinarse las sanciones que se aplicarán a su autor o autores. La pregunta clave a este respecto es si es o no conveniente la introducción en el C. P. de nuevos preceptos que recojan estos comportamientos y establezcan sanciones para los mismos o bien si, por contra, es posible castigar las mencionadas conductas mediante tipos penales ya existentes [48].

Para empezar, consideraré la conducta aisladamente, con independencia de su autor. En mi opinión, atendiendo a las clasificaciones más o menos

---

[45] CAMACHO LOSA, L. «El delito informático». cit. pp.143 y ss.

[46] CAMACHO LOSA, L. «El delito informático». cit. p. 73

[47] ROMEO CASABONA, C. «Poder informático» cit. p. 40 y GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p.83

[48] RIVERO CORNELIO, A.M. «Informática y Derecho. La Informática Jurídica en España». Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12, Monográfico sobre Informática y Derecho, 1986. p.201. Se plantea «si la utilización masiva de los ordenadores y la telemática puede cambiar la naturaleza y el alcance de la conducta delictiva (...) si puede llegar a configurar nuevos tipos de delito y (...) si es necesario dotar a la sociedad de unos medios jurídicos específicos para su protección y defensa».

coincidentes que la doctrina española viene elaborando sobre modalidades de comportamientos delictivos inscribibles en la delincuencia informática [49], estos comportamientos pueden subsumirse en preceptos actuales de nuestro C. P. (falsedades, estafas, hurto, robo, daños...) sin necesidad de crear unos nuevos. Es obvio que la delincuencia informática patrimonial presenta caracteres específicos que la diferencian de la criminalidad patrimonial «clásica»; sin embargo, creo que estas especificidades tienen, predominantemente, un interés criminológico o, desde un punto de vista procesal, afectan a las dificultades de descubrimiento y prueba de los hechos. No me parece que estas características diferenciadoras puedan servir como argumento para la introducción en el C. P. de preceptos en los que se recojan los citados comportamientos. Como apuntaba al tratar de definir la delincuencia informática patrimonial, creo con ROMEO que estamos ante una pluralidad de delitos que tienen, como única nota común, su vinculación con los ordenadores [50]. La nota diferenciadora por excelencia la constituye la concurrencia de un ordenador en alguna o todas las fases de ejecución del delito. No cabe duda de que se trata de un elemento diferenciador muy considerable, pero a pesar de ello no afecta, a mi juicio al contenido básico a la «sustancia del delito» [51], [52]. En todo caso, podría servir de base para la creación de tipos agravados respecto de los básicos ya existentes.

El delincuente informático, por otra parte, no se identifica con la imagen que la opinión pública se ha forjado del delincuente «clásico» contra el patrimonio. Desde este punto de vista se cuestiona la aplicación de sanciones penales a los delincuentes informáticos aludiendo a su «incapacidad de motivación». Sin embargo, respetando siempre el principio de intervención mínima del Derecho Penal, la sanción penal deberá aplicarse cuando sea necesario, también al delincuente informático. Atendiendo en primer lugar al principio de proporcionalidad de las penas, no olvidemos los cuantiosos perjuicios patrimoniales que causan estas conductas, perjuicios que las hacen merecedoras, en mi opinión, de un reproche mayor que el que conlleva la sanción administrativa. Se argumenta también, en contra de la aplicación de sanciones penales a este tipo de delincuentes, que no tienen conciencia de actuar de forma ilícita. No creo que esta sea una característica específica del delincuente informático sino que, por contra, se da en otras muchas manifestaciones de delincuencia. Por otra parte, el hecho de que el control penal sea poco eficaz en este tipo de delincuencia, dada la elevada cifra negra que se

[49] Ver clasificación de GONZÁLEZ RUS, J. J. «Aproximación al tratamiento penal...» cit. pp. 116 y ss.

[50] Ver nota 1.

[51] RUIZ VADILLO. E «Tratamiento de la delincuencia informática» cit. p. 72

[52] Supera el objetivo de esta ponencia el análisis minucioso de cada uno de los comportamientos delictivos llevados a cabo mediante o sobre sistemas informáticos para determinar así en qué precepto del C.P. pueden subsumirse. En este sentido remito a ROMEO CASABONA, C. «Poder informático» cit. desde la p. 47

intuye, no es argumento suficiente para propugnar la no aplicación de sanciones penales, sino para meditar sobre posibles mejoras de los mecanismos de control. Por último, y por lo que respecta a la aplicación de la pena privativa de libertad a estos delincuentes, se ha dicho que ésta no puede cumplir el fin resocializador que le otorga la Constitución en el art. 25.2º , puesto que estos delincuentes no necesitan resocialización [53]. No estoy de acuerdo con esta apreciación. Entiendo por reinserción social la «capacitación para vivir en sociedad sin infringir notablemente las leyes penales» [54], y en este sentido está claro que estos delincuentes necesitan de reinserción social. Hoy en día, ciertamente, el fin resocializador de la pena está sumido en una profunda crisis: la pena no resocializa, «pero no resocializa a nadie. ¿Por qué ha de merecer un régimen discriminatorio este autor?» [55].

Para concluir y a modo de resumen: puede deducirse de las características de los hechos, que el establecimiento de medidas preventivas resulta muy eficaz para evitar la comisión de ilícitos mediante procedimientos informáticos. Una vez cometido el hecho, descubierto su autor y salvadas las dificultades procesales (esto es posible en pocas ocasiones, pero no por ello debe dejar de plantearse el supuesto), deberán aplicarse al autor las sanciones previstas en los preceptos penales en los que sea subsumible su conducta, siempre que ésta, naturalmente constituya delito.

BIBLIOGRAFIA

BAJO FERNÁNDEZ, M. Manual de Derecho Penal. Parte Especial. II. Delitos patrimoniales y económicos. Ed. Ceura. Madrid, 1987. – Derecho Penal económico. Ed. Civitas. Madrid, 1978.

BERISTAIN IPIÑA, A. «Eficacia de las sanciones penales frente a la delincuencia económica». Indice Penale. Ed. Cedam-Padova, 1982.

CAMACHO LOSA, L. El delito informático. Ed. Ministerio de Cultura. Madrid, 1987.

GARCÍA-PABLOS DE MOLINA, A. Estudios Penales. Ed. Bosch. Madrid, 1984.

GONZÁLEZ RUS, J. J. «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos». Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12. Monográfico sobre Informática y Derecho. 1986.

[53] Utilizo el término «resocialización» como sinónimo de «reinserción social». Sobre los problemas que plantea el término «resocialización» véase GARCÍA-PABLOS DE MOLINA, A «La supuesta función resocializadora del Derecho Penal» En Estudios Penales cit. pp 22 a 27.

[54] BERISTAIN IPIÑA, A. «Eficacia de las sanciones penales frente a la delincuencia económica». L. Indice Penale 1982

[55] GARCÍA-PABLOS DE MOLINA, A. «Derecho Penal y criminalidad financiera». En Estudios Penales cit. p. 244. Ver también la nota 139 en la misma página. La palabra «autor» de la frase que transcribo, aunque se refiere al autor de delitos económicos y no propiamente al delincuente informático, creo que resulta trasladable a este contexto.

GUTIÉRREZ FRANCÉS, M. L. Fraude infomático y estafa. Ed. Centro de publicaciones del Ministerio de Justicia. Madrid, 1991.

ROMEO CASABONA, C. Poder informático y seguridad jurídica. Ed. Fundesco. Madrid, 1987.

RIVERO CORNELIO, A. M. «Informática y Derecho: La Informática Jurídica en España». Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12. Monográfico sobre Informática y Derecho. 1986.

RUIZ VADILLO, E. «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica». Poder judicial. Número especial IX. 1988.

TIEDEMANN, K. Poder económico y delito. Ed. Ariel. Barcelona, 1985. «La criminalidad económica como objeto de investigación». Cuadernos de Política Criminal. Número 19. 1983.

Prevención Versus Fraude: La Auditoría Informática

EMILIO DEL PESO NAVARRO
Banco Hipotecario
(ESPAÑA)

Es mejor prevenir los delitos que punirlos.
Cesare Beccaria (De los delitos y las penas).

INTRODUCCION

El pensamiento de CESARE BECCARIA es aplicable, por supuesto, a todo el ámbito del Derecho Penal pero, si cabe, aún más al específico dominio de los llamados delitos informáticos como trataremos de explicar en las líneas que siguen.

En los últimos años el uso de las nuevas tecnologías de la información en las empresas y en las distintas Administraciones ha experimentado un desarrollo espectacular.

En un período de cambio acelerado e intenso, en un mundo, como lo denomina TOFFLER, de la tercera ola o del superindustrialismo (TOFFLER 1985) el gerente, el empresario ha de revisar todas las conjeturas de la gerencia sobre el mundo económico y social que le rodea y esto sólo puede hacerlo disponiendo de una información actual y veraz.

Por ello el empresario, el gestor de nuestros días demanda una información cada vez más actual y elaborada para poder tomar decisiones más rápidas y con menos riesgos.

Dado el volumen de datos que es preciso manejar para elaborar esa necesaria información en un tiempo prudencial antes de que quede obsoleta, ya no son válidos los métodos tradicionales de tratamiento de la información. Es necesaria la utilización de las nuevas tecnologías que permitan ese masivo tratamiento de datos con una alta velocidad de proceso.

El empleo de sistemas más o menos informatizados es usual en la mayoría de las grandes y medianas empresas y con la aparición de los ordenadores personales y los paquetes integrados su introducción en las pequeñas crece rápidamente.

El uso de estas nuevas tecnologías ha generado importantes beneficios, pero también ha creado nuevos riesgos ya que hoy en día la información es uno de los patrimonios más valiosos de la empresa y por ello hay que protegerla contra una amenaza que cada día cobra más fuerza: la utilización de estas nuevas tecnologías con fines delictivos.

Es importante resaltar el gran valor que en nuestra época adquiere la información. Siempre ha sido valiosa, pero en el pasado no existía la posibilidad como ocurre ahora, de convertir informaciones parciales y dispersas en informaciones en masa y organizadas.

RIESGOS POTENCIALES DE LA INFORMACION

Esta importancia acrecienta los riesgos que amenazan a la información y hace que las consecuencias que su pérdida origina puedan llegar a ser catastróficas. En el pasado, por ejemplo, el incendio de la biblioteca de Alejandría fue una pérdida cultural irreparable, pero forzoso es reconocer, como dice el profesor SCALA, que no afectó a la vida política, económica o social de Grecia y Roma. Por el contrario la información que hoy se elabora automáticamente y se archiva en los computadores es algo vivo, cambiante, dinámico y directamente relacionado con la actividad humana. En definitiva es un bien que debe ser protegido, porque su destrucción acarrearía daños a personas e instituciones.

La facilidad de borrado y de reescritura sobre los soportes magnéticos los hacen especialmente sensibles a la alteración, supresión o introducción de datos dejando escasas huellas de la manipulación o la absoluta ausencia de ellas. (Scala 1990).

Para tratar de evitar los riesgos potenciales que el uso de estas nuevas tecnologías en la empresa trae consigo o por lo menos minorizar sus desastrosas consecuencias nace la Auditoría Informática, como veremos mas adelante.

Es importante resaltar la velocidad con que, a diferencia de lo que ocurre en otro tipo de delitos, puede desaparecer la prueba cuando se comete un fraude informático. Desaparición que en algunos casos puede llegar a ser, como se ha dicho, total sin dejar prácticamente ninguna huella.

Esta circunstancia habremos de tenerla necesariamente en cuenta cuando tratemos de implantar algún sistema de prevención.

Existen tres momentos claves en el procesamiento de la información en los que ésta puede ser alterada: en el momento de la entrada de los datos en el sistema, durante el tratamiento de los mismos en esa «caja negra» que es el ordenador, entendido en su más amplio significado, y en la salida de datos del sistema.

Con los sistemas tradicionales de auditoría se pueden verificar la entrada y salida de los datos pero dificilmente se puede comprobar lo que ocurre durante el procesamiento de los mismos.

Para nadie es un secreto que una salida impresa o por pantalla de un terminal puede ser perfectamente «dibujada» a conveniencia de quien lo hace con la posibilidad de falsear la realidad.

La integración de la Informática, en particular gracias a las redes, hace el problema todavía más grave; las consecuencias de una anomalía pueden propagarse al exterior de las empresas e incluso alcanzar a los usuarios individuales. Las implicaciones sobrepasan, por tanto, al simple plano socioeconómico, y alcanzan a la propia ética.

UNA NUEVA FORMA DE DELINCUENCIA

La proliferación en los últimos años de los sistemas informáticos en el mundo empresarial y en el de las diferentes Administraciones Públicas ha propiciado la aparición de una nueva forma de delincuencia. Sin asumir riesgos físicos ni ejercer violencia ahora es posible obtener, de forma fraudulenta, ingentes cantidades de dinero sin dejar rastro y con la seguridad de que en el caso de ser descubiertos se gozaría de una total impunidad al no estar contempladas estas nuevas figuras delictivas en el ordenamiento jurídico español.

Al estudiar esta problemática es muy interesante tener presente la motivación del delincuente informático. Existe un paralelismo entre los motivos para cometer «delitos comunes» y «delitos informáticos» aunque en el segundo caso no esté empleada la palabra delito con propiedad. Los objetivos de ganancia personal causada por necesidades económicas o ganancia institucional para beneficiar a una empresa, o incluso el deseo de venganza en contra de una compañía, aunque por métodos diferentes, son aplicables a ambos tipos de delitos.

Hay, sin embargo, motivos específicos propios de la existencia de los ordenadores. El ordenador se presta al juego de la exploración y con su tecnología es un reto a la inteligencia humana.

No es fácil encontrar estadísticas fiables sobre estos crímenes contra la propiedad y sobre el coste que para las empresas supone esta actividad delic-

tiva, pues al tratarse principalmente de entidades del mundo financiero, no son muy proclives a airear este tipo de información, por el resultado negativo que para el negocio podría suponer la disminución de clientes temerosos de una hipotética falta de seguridad de la entidad.

Objetivo de esta nueva forma de delincuencia son tanto los datos como las diferentes aplicaciones de los sistemas informáticos.

La gravedad del problema es tal que en un futuro se podría llegar a la eliminación por medios informáticos de un competidor, que no estuviese debidamente protegido, creando criminalmente el caos en su sistema informático y originando con ello la desaparición de su empresa.

Perfil del delincuente informático

En el delito que nos ocupa no hay un tipo de delincuente único con características propias y definidas, no existe un «retrato robot» y el panorama es amplio y variado, desde el ratero aficionado, al administrativo furtivo, pasando por el timador casual y por el niñato adolescente y desocupado, hasta llegar al profesional astuto, que emplea medios sofisticados para alcanzar un lucrativo fin. (LAFUENTE 1990).

El delito informático en el párrafo anterior es entendido en un sentido muy amplio.

Es interesante el perfil del delincuente informático que propone Luis Camacho en un dominio más restringido del delito informático y en función de la información recogida en un cierto número de fraudes descubiertos:

-Suele ser empleado de confianza, bien por el tiempo que lleva en la empresa o bien por el tipo de trabajo que realiza.

-Es un empleado que por su trabajo tiene acceso al sistema informático y conoce suficientemente sus debilidades como para permitirle realizar el hecho delictivo.

-En gran número de casos suele ser usuario del sistema y no técnico informático. Es conveniente tener presente que este perfil se ha logrado en función de los fraudes descubiertos, por lo tanto esta afirmación puede ser debida más que a un nivel superior de honradez del colectivo de técnicos, a la posibilidad de que los fraudes que cometen sean más difíciles de descubrir.

-Suele ser una persona que trabaja en solitario o como máximo en grupo de dos o tres personas.

-Carece de antecedentes penales.

-Joven con edades comprendidas entre 18 y 30 años, varón, en su mayoría soltero y sin ataduras familiares.

-Profesional brillante y altamente motivado por su profesión y por el desafio técnico que conlleva. (CAMACHO 1987).

Es conveniente resaltar en este perfil la característica de que el presunto delincuente suele trabajar en solitario, esto viene a confirmar que aún la criminalidad organizada no ha entrado a operar en el mundo informático, lo cual no quiere decir que no lo haga en el futuro.

IMPORTANCIA DEL ESTABLECIMIENTO DE UN SISTEMA PREVENTIVO

El perfil descrito nos lleva a la conclusión de que gran parte de los fraudes informáticos son cometidos desde dentro de las propias empresas bien por empleados que siguen trabajando en la misma empresa, bien por personas que en el pasado trabajaron en ella y por lo mismo conocen su sistema informático.

El establecimiento de un sistema de evaluación informática periódico, en el aspecto preventivo, suele producir efectos positivos inmediatos, pues el conocimiento por parte del personal de una empresa de que se efectúa regularmente una evaluación de este tipo evita en gran proporción la comisión del «delito» informático ante la posibilidad de ser descubierto con facilidad.

Aún más positivo sería el establecimiento de un sistema de evaluación contínuo, que evitaría los tiempos muertos entre una evaluación y la siguiente.

LA AUDITORIA INFORMATICA

Este sistema de evaluación, que con carácter preventivo, se propone en el párrafo anterior en realidad es lo que se conoce como Auditoría Informática.

Para entender mejor lo que es la Auditoría Informática vamos a seguir la definición, muy completa, de RAMOS GONZÁLEZ:

«La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes del entorno informático de una entidad, abarcando todas o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables; el grado de satisfacción de usuarios y directivos; los controles existentes y un análisis de los riesgos.» (RAMOS GONZÁLEZ 1990).

Como vemos uno de los objetivos de la Auditoría Informática, y para nosotros como juristas el más importante, es evaluar la fiabilidad de los sistemas informáticos en cuanto a la exactitud de los datos o información que trata a través de los diferentes controles existentes.

Estas revisiones abarcan no sólo los sistemas implantados sino algo todavía más importante, aquellos sistemas que estan en desarrollo.

En el momento del desarrollo de las aplicaciones se deben prever ya determinados controles que posteriormente puedan ser rastreados por los programas de auditoría.

DIFERENTES ASPECTOS DE LA AUDITORIA INFORMATICA

La Auditoría Informática la debemos, pues, contemplar en sus dos aspectos: como posible medida de prevención, en algunos casos de disuasión, para que algo no ocurra y como medida de fiscalización para comprobar lo que ha ocurrido y en su caso facilitar la necesaria prueba.

El empresario actual debe imitar a aquella casada prudente que antaño elevaba una oración al Cielo a fin de que su marido no la engañase, una segunda para que si la engañaba no llegase a tener conocimiento de ello y una tercera para que si la engañaba y se enteraba no le importase. El empresario debe rogar en primer lugar para que en su empresa, en su sistema informático no se cometa un fraude, en segundo lugar para que si se comete se pueda detectar y en tercer lugar para que si lo anterior ocurre se pueda lograr una prueba del fraude cometido. Nos atrevemos a decir que debería seguir rogando para que el fraude cometido, descubierto y probado estuviese a su vez tipificado como delito en el Código Penal.

Si importante es la labor de prevención, en la que queremos hacer hincapié no lo es menos, cuando ésta fracasa, esa otra labor de fiscalización.

Si en cualquier tipo de delito es importante recoger la prueba del mismo lo antes posible y siempre con anterioridad a su temida desaparición; en el caso del fraude informático esto es vital por la facilidad que existe para que las pruebas sean borradas intencionadamente o sin intencionalidad, simplemente por la dinámica del sistema.

CONCLUSIONES

Lo expuesto anteriormente nos lleva a la conclusión final de que la Auditoría Informática puede perfectamente servir para **prevenir, descubrir y probar** el hasta el momento fraude informático y que esperamos que en un futuro próximo sea delito informático.

La razón por la que en el dominio de los llamados delitos informáticos es más aplicable el pensamiento de Beccaria, mejor prevenir que penar, que en otro tipo de delitos, viene motivada, con independencia de sus derivaciones de tipo filosófico, por la práctica inexistencia de unas normas legales que castiguen los mismos, lo que, a la postre, viene a significar el disfrute de una total impunidad.

Insistimos en que el simple conocimiento de que en una empresa se dispone de las debidas medidas de seguridad en sus instalaciones y se realizan las Auditorías Informáticas precisas, es la mejor medida de prevención frente al fraude informático y la inversión que se realice en este área será una de las más rentables para la empresa.

Es evidente que, poco a poco, el empresario, el gestor va comprendiendo la utilidad y la necesidad de contar con los auditores informáticos.

Los juristas no los debemos olvidar, pues su trabajo nos puede ser de gran utilidad.

De forma inexorable, en un futuro próximo, las empresas que no puedan tener la certeza de que sus sistemas informáticos son fiables, que sus datos responden a la realidad, que no son víctimas de estos nuevos tipos de criminalidad no podrán competir en ese gran mercado del mundo superindustrial que se avecina y tenderán a desaparecer.

Todo esto es trasladable a la diferentes Administraciones Públicas, aunque en éstas, obviamente, el resultado final no pueda ser el mismo.

Quisiera terminar estas modestas líneas con una reflexión del gran pensador español Julián Marías muy apropiada para los que de una forma u otra nos movemos en este fascinante mundo de la Informática:

«Es menester que los que usan la tecnología electrónica no crean que los aparatos piensan por ellos, es esencial que vean que la técnica electrónica da solamente instrumentos para pensar yo, único que puede hacerlo, único que puede saber.(Marías 1985).

BIBLIOGRAFIA

BECCARIA BONESANA C. «De los delitos y las penas». Madrid. *Aguilar* 1969. 121 pp. (p. 180).

CAMACHO L. «El delito informático». Madrid 1987. 162 pp. (p. 84).

LAFUENTE J. J. «Conozca las artes de los delincuentes informáticos». Estrategia Financiera núm. 57, 1990. (p. 22).

MARÍAS J. «Cara y Cruz de la Electrónica». Espasa Calpe. Colección Austral. 1985. 103 pp. (p. 99).

RAMOS GONZÁLEZ M. A. «Contribución a la mejoría de las técnicas de Auditoría Informática mediante la aplicación de métodos y herramientas de Ingeniería del Conocimiento». Tesis Doctoral. Madrid Universidad Politécnica 1990. 119 pp. (p. 17).

SCALA ESTALELLA J. J. «Validez legal de los documentos generados por sistemas automáticos». Encuentros sobre Informática y Derecho 1990-1991. Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE). Pamplona. *Aranzadi* 1992. (p. 11).

TOFFLER A. «La empresa flexible». Espluges de Llobregat. Plaza y Janés 1990. pp. 220 (p. 103).

Criptología; Seguridad Informática y Derecho Leyes del Ciberespacio

MIGUEL A. GALLARDO ORTIZ

Ingeniero Superior de Minas, especialidad de Energía y Combustibles. Consultor Profesor de Unix & C.

(ESPAÑA)

La criptología es una elegante disciplina matemática con una fascinante historia y un prometedor futuro en el mundo de la informática y las comunicaciones digitales modernas.

Los algoritmos criptológicos representan, directa o indirectamente, el único procedimiento conocido para garantizar la confidencialidad y la autenticidad de la información, mediante la clave secreta y la firma electrónica.

Además de una breve, aunque sólida introducción técnica a la criptología moderna, y métodos de control de acceso, protección frente a actos vandálicos (virus y hackers), y monitorización del trabajo informático colectivo, el profesional del derecho informático debe tener conocimientos sobre cómo se contemplan en la legislación española, europea, y de países avanzados en este área como los EEUU y Japón.

La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y algunos artículos del proyecto de nuevo Código Penal, así como las normativas y leyes de menor rango que comienzan a tratar, con sus luces y sus sombras este nuevo fenómeno, darán lugar al desarrollo de una industria, y de unos contenciosos, entorno al delito informático.

Pero además, la ética del secreto, y su representación en el ordenador y transmisión por medio de enlaces telemáticos van a cambiar la conciencia

colectiva respecto al uso y al abuso de la información en una sociedad que cada vez está más cerca de ese modelo postindustrial que algunos autores han llamado infoesfera y otros ciberespacio, en los que se consigue la eliminación virtual de las distancias. Es aquí donde está, sin ningún género de dudas para nosotros, la más apasionante aventura intelectual de los tiempos en que nos ha tocado vivir.

FUNDAMENTOS DE CRIPTOLOGIA PARA PROFESIONALES DEL DERECHO

Como es bien sabido, la criptología es casi tan antigua como la escritura y, hasta el reciente desarrollo de la informática, ha estado al servicio exclusivo de los grandes poderes políticos y económicos. El cifrado de la información solía ocultar secretos de estado, o servir de cauce a comunicaciones militares.

Es previsible que, en España, la promulgación de la Ley Orgánica para la Regulación del Tratamiento Automatizado de los datos de Carácter Personal (LORTAD) provoque una rápida sensibilización de Administración y de empresas, especialmente en algunas actividades que hasta ahora se han ejercido con la mayor impunidad, y en ocasiones, fraudulentamente.

Actualmente, los más modestos sistemas informáticos son capaces de realizar complejas encriptaciones o cifrados de información, y lo único que queda en manos de los grandes poderes políticos y económicos es la remota posibilidad de intentar un acceso no autorizado, aunque para ello tengan que dedicar durante meses costosos ordenadores vectoriales tipo Convex, Fujitsu VP o Cray. Muchos más escasos aún son los especialistas capaces de ofrecer unas mínimas garantías de éxito en el ataque. Y desde luego, España no es una potencia en la Guerra Electrónica.

A continuación, describiremos brevemente el «state of the art» en esta estratégica tecnología, así como las instituciones que en España se dedican a tan fascinante disciplina y los acontecimientos que últimamente han estado estrechamente relacionados de una u otra forma con criptología.

TECNICAS MAS EMPLEADAS EN LA ACTUALIDAD

La microelectrónica ha hecho posible la rápida ejecución de programas con complejos algoritmos, pero todavía se siguen utilizando las series aleatorias, que básicamente consisten en una larga serie de números aleatorios (o pseudoaleatorios) a modo de libreta de uso único para el cifrado y descifrado de mensajes, y con una clave tan larga como el texto a cifrar. Aunque es bastante seguro, este método obliga a realizar complejos intercambios de claves y no aprovecha los recursos que ofrecen actualmente la microelectrónica.

Los métodos de cifrado más utilizados en la actualidad son los de clave privada, como el DES, pública, como el RSA, y se está experimentando con una nueva generación de algoritmos basados en curvas elípticas de la forma: $y^2 = x^3 + a\,x + b$

El gobierno de los Estados Unidos ha sido particularmente estricto a la hora de impedir la exportación de criptología, al igual que ha hecho con los ordenadores vectoriales y la fotónica.

En particular, el término Data Encryption Standard o DES no suele emplearse correctamente fuera de los EEUU, ya que el National Bureau of Standards no extiende el certificado de homologación a sistemas no americanos salvo en casos muy excepcionales. Parece ser que consideran que su divulgación puede afectar al modo de vida norteamericano, ya que ni ellos mismos serían capaces de descifrar las comunicaciones en las que se utiliza. Y hemos tenido ocasión de comprobar recientemente todo lo que los EEUU están dispuestos a hacer para protegerse.

El Data Encryption Algorithm o DEA, es el que una vez homologado proporciona el DES, y no es difícil conseguir alguna versión en C portable a MS-DOS, Unix, VMS, etc. Consiste en 16 pasos de sustitución y permutación de bits, y produce un mensaje cifrado tan aleatorizado que es prácticamente imposible obtener el texto legible si no se conoce la clave. Es mucho más eficiente si se ejecuta en un hardware orientado a la criptología, como el que suministra Intel, AMD o Motorola cuando disponen de información suficiente del usuario final.

Al igual que ocurre con el resto de los algoritmos considerados como seguros, también existen rumores de que se ha conseguido desarrollar un procedimiento de ataque al DES con grandes posibilidades de éxito. Sin embargo, nadie lo ha hecho público hasta ahora, y quien lo hiciera sin duda pasaría a la posteridad, ya que la inversión realizada mundialmente en tecnología DES es muy considerable, y cualquier técnica que cuestionase su seguridad provocaría medidas drásticas en el mundo financiero, político y diplomático de nuestros días.

La principal alternativa al DES es el RSA, que permite no sólo encriptar, sino también autentificar los mensajes. Los sistemas de clave pública como RSA se utilizan dando a conocer el método de cifrado y manteniendo en secreto el de descifrado, de forma que si A quiere mandar un mensaje cifrado y autentificado con su firma electrónica, lo que debe hacer es cifrarlo con el procedimiento que B publica, y descifrarlo con el suyo propio, de forma que cuando le llegue a B, éste pueda descifrarlo con su procedimiento y comprobar que proviene de A probando a cifrarlo con su procedimiento. Naturalmente, debe ser imposible deducir el método de descifrado aunque se conozca el de cifrado.

La seguridad del algoritmo RSA se basa en lo inabordable que resulta la descomposición factorial de grandes números formados por el producto de números primos también grandes. Incluso si se utilizase el más moderno Cray YMP, Convex C3, Fujitsu VP o Nec con varios procesadores vectoriales (tal vez los hipercubos o multiprocesadores con paralelismo masivo algún día los superen), es decir, con una potencia de cálculo de muchos MFLOPs, serían necesarios muchísimos años para descomponer en factores primos el producto de dos números primos de 150 dígitos cada uno. Aunque es previsible la aparición de sistemas órdenes de magnitud más potentes que los actuales, desde el punto de vista matemático resulta muy difícil mejorar la eficiencia de los algoritmos de ataque empleados actualmente.

Un desarrollo original para sistemas Unix y MS-DOS en el que actualmente estamos comprometidos es en el que se basa en lo que hemos denominado como «defensa activa». Se trata del Proyecto Pandora (X86), y consiste en comprimir y encriptar los datos fusionándolos con el programa desencriptador descompresor en un sólo ejecutable capaz de destruirse o de intoxicar en el caso de que se intente un acceso no autorizado.

CRIPTOLOGIA AQUI Y AHORA. EN EL ALMA DE UNA NUEVA EMPRESA

Probablemente, España sea uno de los países en los que las técnicas de seguridad empleadas guarden menos relación con el valor de la información que se protege. Podemos asegurar que hay mucho más morbo que economía, industria o inteligencia.

Mientras, Ejército y CESID dedican generosos presupuestos a proteger información prácticamente ociosa (a pesar de que hay agujeros que no serían difíciles de encontrar en sus sistemas), otras instituciones como la Policía o el Ministerio de Asuntos Exteriores ofrecen demasiada facilidad para acceder a información que, si no está clasificada, sin duda debería de estarlo.

Y lo que es peor, la capacidad de criptoanalizar información codificada de nuestros cuerpos y fuerzas de seguridad del Estado ha sido desafiada por la organización terrorista ETA. Parece ser que, rodeado de un cierto secretismo, los ordenadores requisados no han podido ser desprotegidos hasta el momento.

Desde el punto de vista académico, si bien se imparten unas nociones de criptología contempladas en los programas varias de escuelas de ingeniería y facultades, sólo en la Facultad de Informática de la Universidad de Granada existe actualmente una asignatura cuatrimestral con el nombre de «Criptología».

Desde Edgar A. Poe, y Alan Turing, ninguna persona o institución se autocalifica seriamente como experto en criptología inversa o criptoanálisis, aunque sí que se admiten algunas apuestas. En España se ha alquilado por

varios cientos de millones de pesetas anuales un potente ordenador vectorial que, según cabe deducir por las especificaciones técnicas que se formularon hace menos de dos años por parte de Defensa-INTA, parece destinado al menos a intentar el criptoanálisis, aunque no va a ser fácil realizar proyectos propios comparables a los de otros centros de la OTAN, mucho más por la falta de medios humanos, que materiales.

Como curiosidad, me permito dar a conocer que quien escribe esta comunicación ha tenido la gran satisfacción de colaborar con el autor de un elegante y eficaz criptoanálisis del programa de encriptación que WordPerfect ofrece a sus confiados usuarios en la opción Ctrl+F5 (Contraseña). Ahora podemos averiguar en segundos la palabra secreta con la que se ha protegido un documento WordPerfect independientemente de la versión, sistema operativo y hardware con el que se haya elaborado.

Tanto este curioso criptoanálisis, como los detalles del diseño del anteriormente mencionado proyecto Pandora, programa autodestruible–comprimible–encriptable–intoxicador, fueron expuestos en una ponencia que presentamos en la I Reunión Española sobre Criptología, celebrada en Palma de Mallorca del 2 al 4 de Octubre con el patrocinio del Gobierno Balear.

En dicha Reunión, organizada por el Laboratorio de Criptología del CSIC y la Universitat de les Illes Balears participaron responsables de la seguridad de la información de diversas instituciones públicas y privadas, así como varias empresas que ofrecen productos y servicios en un mercado del que se dice que todavía no ha visto la quiebra de ninguna empresa especializada en tan sensible y a la vez desconocida materia en España.

ZERO KNOWLEDGE PROOF. LA SOMBRA DE UN SECRETO

Muchas de las más brillantes ideas que pueden aplicarse en criptología son útiles también en las más variadas esferas profesionales. Pero pocas son tan elegantes como las pruebas con conocimiento cero.

El problema de la identificación segura es uno de los más apasionantes a los que se enfrenta tanto la informática como las comunicaciones digitales modernas. En esencia, cualquier sistema ha de asociar un identificativo (login) y un número secreto (password) a cada usuario autorizado.

Sin embargo, en los sistemas en los que se deposita información altamente confidencial, las suspicacias, y también la experiencia, aconsejan no revelar el número secreto ni siquiera al administrador o responsable del sistema.

¿Cómo puede verificarse entonces la autenticidad de la identidad que el usuario declara?

Pensemos en un matemático que descubre una nueva teoría con la que consigue explicar satisfactoriamente algunas observaciones o fenómenos.

Este matemático no desea dar a conocer la parte fundamental de su teoría, pero quiere convencer al resto de la comunidad científica de que la ha descubierto únicamente él, y de que es correcta.

La teoría del Zero Knowledge Proof consiste, básicamente, en elaborar un protocolo mediante el cual otros científicos hacen preguntas concretas al descubridor de la teoría secreta, y éste les responde con el conocimiento del secreto, pero sin dar detalles de él, hasta convencer a los demás de que sólo es posible la respuesta a las preguntas mediante el conocimiento de un secreto que los demás no poseen.

Para ilustrar gráficamente esta teoría, se recurre a la imagen de un secreto apantallada por una mampara que impide que el público lo vea directamente, pero de forma que dicho secreto pueda ser iluminado desde distintos ángulos. Los espectadores podrían llegar a tener la certeza de que, efectivamente, tras la mampara se esconde el secreto, y que éste es auténtico.

Matemáticamente, todo password o clave puede codificarse como un número entero de tantas cifras como sea necesario. La sombra de un password no sería más que el resto de dividir dicho entero secreto por un número menor que él.

Al igual que ocurre con el algoritmo RSA, los matemáticos especializados en teoría de números trabajan afanosamente tanto por proponer, como por comprobar y rebatir los detalles de los sistemas que se basan en este principio.

Ejemplos de complejas operaciones logísticas, tácticas y estratégicas basadas en el Zero Knowledge Proof son fáciles de encontrar en el terreno militar y diplomático y por supuesto, en las relaciones que mantienen servicios y sociedades secretas con la población ajena a sus intereses.

Pero también el mundo comercial y financiero conocen desde hace mucho tiempo que la información innecesaria que uno proporciona siempre acaba llegando, de la forma más perjudicial, al último interesado en ella, normalmente un adversario o competidor.

Y por supuesto, un buen abogado debe conocer los fundamentos del Zero Knowledge Proof, aunque sólo sea de una forma intuitiva, para realizar su trabajo cotidiano sin perjudicar a sus clientes.

CONTENCIOSOS INFORMATICOS ACTUALES, Y VICTIMIZACION SECUNDARIA

A lo largo de este último año se han visto en los tribunales tres casos en los que la información accesoria ha sido la clave de procesos de victimización secundarios.

El primero de ellos ha sido el escándalo de la red de tráfico de datos, en el que el interés, el lucro, la ignorancia y la pereza periodística han alejado la atención informativa de la verdad.

El segundo ha sido el del pirata informático que ha «robado» 12.000 millones a no se sabe quien. Sólo encubierta por una supuesta operación antidroga se pudo proceder al registro.

Y por último, un importante banco está siendo inspeccionado informáticamente en estos momentos, y al igual que en los casos anteriores, existen serias dudas sobre segundos o terceros usos que puedan hacerse de las órdenes de un juez.

De lo que no cabe ninguna duda es que si no escribimos nosotros las reglas de la justicia informática, alguien lo hará por nosotros, probablemente en inglés, y por bien que se traduzcan, será difícil salir beneficiados aquí con las de otros países.

Los Delitos Informáticos en el Derecho Español

MIGUEL GÓMEZ PERALS
Profesor en la Facultad de Derecho y en la Escuela Universitaria de Empresariales de la Universidad de la Laguna.
(ESPAÑA)

SUMARIO

INTRODUCCION
CONCEPTO
CARACTERES
SUJETOS ACTIVO Y PASIVO
SUPUESTOS DE DELINCUENCIA INFORMATICA
MEDIOS COMISIVOS
COMISION, PERSECUCION Y PREVENCION
DERECHO COMPARADO
TIPICIDAD DE LOS SUPUESTOS DE DELINCUENCIA INFORMATICA
EPILOGO
BIBLIOGRAFIA

INTRODUCCION

En las postrimerías del siglo XX en que nos encontramos se produce el tránsito de la llamada «era de la imprenta» a la de la «informática». La irrupción de esta novedad tecnológica plantea enormes posibilidades a la vez que serios problemas jurídicos. Y ello porque los avances técnicos son sus-

ceptibles de utilizarse no sólo como instrumentos de progreso humano sino de dominación y explotación de los hombres entre sí.

Aunque sería prolijo enumerar las ventajas que conlleva la Cibernética, destaquemos la simplificación y economía que supone la automatización de múltiples operaciones mecánicas –antes desarrolladas manualmente– la celeridad y el aumento de la eficacia de los servicios informatizados.

Por contra, se ha criticado, la aparición de ciertos fenómenos indeseables como el aumento del paro y la propia delincuencia informática. Baste a estos efectos recordar la polémica sobre la bondad o maldad moral de la energía nuclear, en principio aséptica como tal fenómeno científico. Pero como desgraciadamente el progreso técnico no avanza parejo con el desarrollo moral del hombre, a cada adelanto tecnológico le acompaña una específica picaresca cuando no una auténtica morfología delictiva como es el caso de la delincuencia informatica.

Aceptada la interdependencia entre el nivel de evolución tecnológica, el grado de desarrollo económico y social y las manifestaciones criminales, nos adentraremos en el estudio de la delincuencia informática.

CONCEPTO

A pesar de que no existe unanimidad en la doctrina, respecto a qué se entiende por Delincuencia Informática, es preciso el establecimiento de alguna definición –por perfectible que sea– para poder delimitar el objeto de nuestro estudio.

Así, con criterio ecléctico y amplio podemos conceptuarla como el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto –doble vertiente que después examinaremos– a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. O centrándonos más en el aspecto patrimonial: el conjunto de acciones dolosas que provoca un perjuicio a personas físicas o entidades, sin que sea necesario que ello conlleve un beneficio material para su autor, o viceversa, produce un beneficio ilícito para su autor aun cuando no perjudique de forma ostensible a la víctima.

Hemos de hacer sin embargo una precisión terminológica: la expresión «delitos informáticos» es utilizada en este estudio en un sentido impropio, pues no existiendo legislación que tipifique todavía estos supuestos, no puede hablarse de auténtico delito.

El ámbito de incidencia de la Delincuencia Informática, o dicho de otro modo los bienes jurídicos que constituyen su objetivo son cada vez mas variados: la esfera privada de la personalidad del ciudadano –lo que los anglosajones denominan «privacy»–, y su esfera patrimonial: campos ambos a que

nos referiremos en este comentario. Ello sin perjuicio de que en otras ocasiones las conductas afectan intereses públicos (seguridad del Estado, datos administrativos, etc.)

Más concretamente la intimidad y dignidad de la persona física, se ven lesionadas cuando datos relativos a los aspectos más variados de su existencia (profesionales, económicos, sanitarios,) son almacenados, consultados, transmitidos y utilizados no siempre para los fines que justificaron la creación del fichero en cuestión, o por personas diferentes de las autorizadas para ello.

Por otra parte, el segundo bloque de bienes jurídicos afectados por esta forma de criminalidad son los patrimoniales en sentido estricto, referidos a los derechos e intereses económicos y financieros (cuentas corrientes, percepciones por dividendos o pensiones, etc).

CARACTERES

Respecto de su encuadre doctrinal ya hemos dicho que la Delincuencia Informática puede considerarse como una sección de la llamada «delincuencia económica»; para algunos autores incluso un subgrupo de la de «guante blanco.» Aunque ello no es siempre exacto dado la pluralidad de bienes jurídicos que pueden ser afectados, sí resulta cierto de los supuestos cometidos mediante medios informáticos de los cuales vamos a comentar sus principales rasgos por ofrecer mayor interes que los casos en que dichos medios informáticos constituyen el objeto material de la acción.

Para determinar los principales rasgos que permitirían construir una categoría con los dispersos delitos informáticos es preciso atender tanto al sistema económico y al contexto social en que tienen lugar, como a las propias características tecnológicas de la Ciencia Informática.

Una nota sociológica interesante de la Delincuencia Informática es la escasa publicidad que se le da por la víctima, principalmente entidades bancarias, para no provocar su desprestigio y la desconfianza de sus clientes. El porcentaje de las llamadas «cifras negras» en esta delincuencia es muy alto. Los delitos son descubiertos generalmente por denuncias anónimas o simple casualidad. Las informaciones verbales son inoperantes no sólo por la falta de pruebas contra el presunto autor sino por la virulenta reacción de éste para evitar su deshonra provocada por la acusación.

Desde el aspecto económico, la «rentabilidad» de estos delitos se calcula que es una tercera parte superior a la de cualquier otro tipo, ya se trate de una o pocas ocasiones en que se sustraen grandes cantidades o de infinidad de operaciones por un importe mínimo (técnica del salami). La lesividad de estas acciones se acentúa porque hoy en día la interconexión entre las actividades económicas genera un efecto de «cascada» en que se ven afectadas multitud de entidades, por lo que el perjuicio aumenta considerablemente.

Por ello resulta especialmente difícil la cuantificación de este perjuicio, pero desde luego suele existir una gran desproporción.

Desde el punto de vista técnico son rasgos decisivos el cáracter incorporal de algunos elementos de la Informática (software), la posibilidad de acumular un ingente caudal de datos en volúmenes reducidísimos (bases de datos), la práctica desaparición del factor distancia o espacio (gracias a las redes de comunicaciones), la reducción alucinante del factor tiempo en la realización de cálculos y procesos complejos. La posibilidad de alterar programas y datos sin dejar rastro dificulta enormemente el hallazgo de pruebas. La complejidad técnica de la materia reduce su conocimiento a un circulo reducido de expertos, respecto de los cuales también resultarían inútiles los controles del sistema. Respecto de esto último nos podríamos plantear el eterno problema: ¿Quién controla al controlador?.

Un rasgo común a estas figuras desde el punto de vista de su punición es la posible consideración de la multa impuesta por el fraude –en los supuestos cometidos mediante medios informáticos– como uno más de los gastos de explotación, por lo que la función preventiva debe actuar también a través de efectivas medidas de seguridad.

La creciente interconexión y trasmisión interfronteriza de datos ha puesto de manifiesto como este fenómeno afecta de modo semejante a los países de un mismo entorno tecnológico.

La internacionalización del problema hace cada vez más necesaria la cooperación interestatal tanto administrativa como judicial para la investigación y prueba de estos delitos. Existen ya trabajos como la Recomendación del Consejo de Europa R (81) 12, a cargo de los Profesores BOLLE y TIEDEMANN, que reflejan la creciente preocupación supranacional por el tema.

SUJETOS ACTIVO Y PASIVO

Respecto del sujeto activo nos centraremos en los posibles autores:

–Los operadores, programadores u otros sujetos en legítima relación con la elaboración del programa. Las personas autorizadas actuan ilícitamente cuando se extralimitan.

–Cualquier persona a través de terminales publicas o interceptando líneas de transmisión de datos a distancia, o bien causando daños a los medios informáticos, ya sean empleados descontentos o activistas con móviles políticos o ideológicos. Son terceros o extraños.

–Los titulares legítimos del sistema, por título de propiedad y por cualquier otro título que les habilite para el disfrute de dicho sistema informático. Resulta curioso cómo la utilización ilícita por los titulares suele ser medio de comisión de otros delitos como el alzamiento de bienes mediante la crea-

ción de doble contabilidad. En este apartado incluiríamos la inutilización de programas por su propietario cuando se dan determinadas circunstancias.

El retrato robot del delincuente informático seria el de un varón, relativamente joven, profesional competente en técnica informática o bien antiguo empleado o usuario que por su trabajo o por la confianza que la empresa ha depositado en él, tiene acceso al sistema informático y conoce sus deficiencias.

También puede ocurrir que el delito se comete por persona jurídica a través de sus órganos. Orillemos la polémica cuestión de la responsabilidad penal de esta clase de personas que es diferente de la de las personas físicas ejecutoras de la acción y de su responsabilidad civil subsidiaria. Y mencionemos sólo algunas medidas punitivas que pueden imponerse: desde la advertencia o caución de buena conducta, confiscación de ganancias obtenidas, prohibición de ejercer determinadas actividades relacionadas con la informática, prohibición de obtener beneficios de naturaleza pública, hasta su cierre.

En cuanto al sujeto pasivo comprende tanto los titulares y demás beneficiarios legítimos del sistema, como los usuarios y terceros de buena fe. La fisonomía típica de la víctima informática es la de una empresa con escaso o nulo nivel de seguridad informática, en que se procesan transacciones que suponen movimientos de fondos y con personal descontento.

SUPUESTOS DE DELINCUENCIA INFORMATICA

Dada la variedad de estos supuestos, es imprescindible su clasificación para su estudio con un mínimo de rigor científico. A su vez, esta clasificación puede hacerse siguiendo diversos criterios.

Uno de ellos es el de atender a la función que el sistema informático –sus elementos o procedimientos– desempeñan en dichos delitos informáticos: el de objeto material de la conducta o el del instrumento que auxilia la acción típica. Así se distinguen dos grupos: los ilícitos patrimoniales contra elementos informáticos y aquellos otros cometidos por medio de procedimientos informáticos. Con independencia de esta distinción surge otra: la que diferencia –respecto al sistema informático– aquellas conductas que afectan a los elementos materiales o «hardware» de aquellas otras que se relacionan con el material lógico o software.

Ilícito contra elementos del hardware informático.

Podríamos citar el hurto, robo o apropiación indebida de un ordenador, incluso su inutilización o destrucción, figuras todas ellas a las que se podrían aplicar perfectamente las reglas propias de los elementos ordinarios no informáticos. Especial interés en temas informáticos presenta el llamado hurto de «tiempo–máquina» que la doctrina considera atípico como tal hurto de uso,

por lo que de momento sólo cabría la reclamación por vía civil de la correspondiente indemnización.

La destrucción, menoscabo o inutilización del hardware podría reconducirse a los delitos de incendio (547 y ss. del Código Penal), estragos (554 y ss.) y daños (557 y ss.) supuestos estos que se diferencian por su respectivo medio comisivo, siendoles común por el contrario la falta de un ánimo –por lo menos inmediato– de enriquecimiento y la intención de causar un perjuicio patrimonial.[1] Respecto de los daños es interesante la circunstancia de una inutilización o pérdida de su operatividad original sin implicar necesariamente destrucción física o pérdida de su sustancia, por lo que queda demostrado una vez más que el detrimento de valor económico de un bien puede recaer sobre la sustancia material o sobre la funcionalidad de su uso. Todo ello sin perjuicio de la tipificación de estas conductas como delito o falta dependiendo de las cuantías previstas en el Código.

Ilícito contra el software informático

La acción recae sobre la información o conjunto de datos almacenados en el diskette o memoria, sin que resulte alterado físicamente ninguno de los elementos del Hardware, o por lo menos sin que sea necesaria dicha alteración física, aunque pueda concurrir. La doctrina distingue varios supuestos:

–El «apoderamiento» de ficheros informáticos (copia con simultánea destrucción del original), hipótesis esta que plantea el siguiente problema. Aceptemos el concepto de cosa corporal mueble como todo objeto mueble o inmueble, aprehensible, susceptible de fundamentar un derecho real de propiedad y valuable en dinero. Este concepto sera coherente con la idea de «tomar o apoderarse» en que se basa la idea clásica de apoderamiento. Pero no parece aplicable a los elementos lógicos o software, salvo que el tipo se configure como desplazamiento patrimonial y no material.

Y ello porque el software está caracterizado como antes dijimos por su inmaterialidad; es en realidad una especie de flujo electro-magnético, por lo que su protección penal podrá asimilarse a la del flujo de energía–eléctrica en los arts 536 y ss. del Código Penal. Sin embargo, esta tesis de las defraudaciones es criticable puesto que en los programas informáticos la relevancia corresponde al contenido de instrucciones y datos y no al consumo ilícito de flujo de energía, que actúa sólo como vehículo de aquel contenido.

Pero si bien los ficheros informáticos no parecen susceptibles por sí mismos del delito del apoderamiento clásico, sí que lo podrían ser cuando el delincuente se apodera del soporte físico que contiene aquel fichero.

Tampoco la estafa encaja bien en estos supuestos. Y no tanto por aquella objeción del concepto de cosa corporal sino por no admitirse que el engaño

[1] Para un análisis más detenido de la posible aplicación de estos tipos a las acciones informáticas, vid. ROMEO CASABONA, «Los delitos de daños en el ámbito informático». Cuadernos de Política Criminal, núm. 43, Madrid 1991, págs. 97 y ss.

–requisito imprescindible en ese delito– pueda darse con respecto a una máquina, en este caso el ordenador. Algun autor considera que esta objeción es artificial: el engañado sería el sujeto titular de dichos objetos.

–Copia sin destrucción del original, supuestos de acceso a la información que la doctrina relaciona con las siguientes figuras:

a) Descubrimiento y revelación de secretos (Arts 497 a 499 a.i.) comprendiéndose tanto los supuestos en que el apoderamiento de papeles o cartas tiene lugar para descubrir secretos como también para obtener un lucro; por persona autorizada (en el caso especial de tratarse de funcionario público véase arts 367 y 368) o no autorizada. Aquí se plantea el problema de interpretación doctrinal de si la expresión «papeles o cartas» puede comprender los ficheros informáticos, como en efecto parece coherente con el actual tratamiento de fotografías y cintas magnetofónicas como medio de prueba.

b) Competencia ilícita, regulada en la antigua Ley de 1902 y en la actual de 1989.

c) Propiedad intelectual, regulada en la antigua Ley de 1879 y la actual de Ley 22/1987 de 11 de Noviembre, así como en la Ley Orgánica de Modificación del Código Penal 6/1987 de igual fecha que retoca los arts. 534 y ss. de este cuerpo legal. El paradigma sería el «pirateo» de un programa.

Completando a los anteriores, el supuesto de copia de un fichero en papel que se puede configurar, si se desprecia el valor del papel utilizado, como un hurto por el valor del fichero.

–Destrucción o inutilización de ficheros; sin embargo el delito de incendio afectaría a los elementos físicos, por lo que parece mas apropiado el delito de daños para proteger el software en sí. Considera Romeo Casabona en el artículo citado [2] que nuestro Código no exige la corporeidad del objeto dañado, precisamente porque la acción de dañar no supone la traslación de un patrimonio a otro, como sería típico de los delitos llamados por ello de enriquecimiento. Por el contrario, el art. 557 del Código Penal solo se refiere a dos notas: que se trate de un objeto de propiedad ajena y que el supuesto no esté comprendido en los delitos de incendio y estragos.

Romeo Casabona resuelve varias cuestiones a cuyo análisis nos remitimos. Baste mencionar que respecto del tipo objetivo se admite la conducta omisiva y en cuanto al tipo subjetivo, lo más frecuente es la exigencia de dolo. Otro aspecto sería la delimitación entre actos preparatorios, tentativa y consumación [3].

La consumación en el delito de daños se determina por la producción efectiva de la destrucción o inutilización, admitiéndose las formas imperfectas de ejecución. Quizá el ejemplo más práctico sea determinar si la introduc-

[2] Op. cit. págs. 104 y 105.
[3] Op. cit. págs. 109 y 110.

ción de una rutina destructiva en el programa constituye un acto ejecutivo punible (tentativa) o uno preparatorio impune.

Parece que la cuestión estriba en que el autor conozca el cuándo y el sí de la activación del mecanismo. Si conoce si se va a producir la activación del mecanismo destructor aunque no sepa cuándo –a fortiori si lo sabe– estaremos ya ante actos ejecutivos; si el resultado no se llega a producir por descubrimiento por el potencial perjudicado, apreciaremos tentativa.

En cambio si el autor conoce el cuándo pero no el sí porque esto depende de un evento ajeno (actuaciones de terceros) estaremos ante actos preparatorios impunes –con mayor razón si ni siquiera conoce el cuándo–. Desde que se produzca dicho evento, es decir, se conozca el sí, empieza el peligro para el bien jurídico pudiéndose y la fase de tentativa pudiéndose dar también el desistimiento hasta terminar en la consumación.

Claro está que si se conservaran copias de seguridad idénticas a las destruidas, el delito habría que apreciarlo en grado de tentativa.

Otro tema interesante que ya apuntábamos al hablar de la autoría es el de la inutilización del programa de ordenador por el titular de los derecho de explotación. [4] El caso más frecuente es el de la empresa comercializadora de software que introduce en los programas vendidos o cedidos rutinas que operarán ante ciertas circunstancias como la falta de pago o la reproducción no autorizada del programa en cuestión. El primer escollo que encontramos para encajar este supuesto en el tipo de daños es que nuestro Código exige la ajeneidad de la cosa objeto del delito, salvo el caso del 562 relativo a daño en cosa propia de utilidad social o economía nacional. Y en el ejemplo citado los derechos de explotación, sino la propiedad intelectual, permanecen, salvo pacto, en la empresa suministradora, obteniendo el cliente sólo el derecho de uso. Los que consideran que no es aplicable el tipo de daños, piensan que la cuestión quedará relegada al ámbito civil por incumplimiento de las respectivas obligaciones contractuales. Otros creen que si bien no son propiedad del cliente de aquellas empresas las instrucciones del programa, sí lo son los datos con él procesados y que por lo menos en cuanto a éstos sí sería aplicable el tipo de daños.

También se ha planteado si sería alegable por dichas empresas la eximente de legítima defensa para justificar aquella introducción de rutinas destructivas. Parece que el impago por el cliente no tendría la consideración de agresión ilegítima y por tanto no sería aplicable tal eximente. Respecto de la otra circunstancia la reproducción no autorizada del programa cedido, si bien constituye una agresión ilegítima, típico supuesto de derecho de autor, lo cierto es que sólo parcialmente procede la aplicación de la eximente por la razón de que en el estado actual de la técnica no parece necesario racional-

[4] Op. cit. págs. 111 y 112.

mente el medio empleado –la destrucción de los datos– para impedirla o repeler dicha copia.

Los ilícitos patrimoniales realizados «por medio» de sistemas informáticos.[5] Su auge se debe a la creciente informatización de las operaciones comerciales, bancarias y bursátiles, fenómeno llamado Transferencia Electrónica de Fondos. Las conductas más características en este ámbito son defraudaciones que se cometen mediante la introducción de datos falsos o la alteración de programas para determinar la transferencia automática, ingreso, o reconocimiento de créditos en favor del autor. Un caso típico sería el pago de pensiones a favor de personas en realidad fallecidas ya, o el redondeo de céntimos en las nóminas o intereses en favor de una cuenta del autor.

Podría reproducirse aquí lo dicho antes respecto de la consideración de cosa corporal imprescindible para la configuración del apoderamiento. Y ello porque la «moneda escritural o moneda de giro» no es una cosa mueble, sino sólo representación de una deuda de valor generada por el traspaso de un crédito de una cuenta corriente a otra, mediante un asiento contable.

Otro elemento del fraude informático sería el perjuicio causado que puede ser económico (dinero, mercancías, valores negociables, servicios) de fácil cuantificación; o inmaterial (prestigio) de mas difícil determinación cuantitativa.

Aún admitiendo este «hurto bancario» habría que considerar que el momento de su consumación es el de la práctica del asiento contable y no en el de la extracción a través de la cual el autor se apodere del dinero físico. Y ello porque ya desde el primero de estos dos momentos el sujeto activo tiene la disponibilidad de la «cosa».

Otro argumento para calificar esta figura de hurto y no de estafa es que así califica la doctrina las maniobras físicas de astucia sobre las cosas, pues a las máquinas no se les puede engañar. Y ello contando con la existencia de perjuicio patrimonial.

También merece examinarse el supuesto de falsificación de documento privado con perjuicio de tercero o con ánimo de causárselo (306 C.P). La objeción en este caso sería la de considerar «documento» los datos recogidos en un soporte informático (diskette, por ejemplo) porque no serían directamente legibles por el hombre.

No puede faltar una somera referencia al tema de los abusos perpetrados en los «cajeros automáticos». Según sea el supuesto de hecho la calificación penal difiere. Distingamos básicamente si la extracción la realiza el titular de la tarjeta o un extraño.

---

[5] González Rus Juan José, «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos». Poder Judicial. Número Especial IX, págs. 48 y ss.

Así, en las extracciones repetidas en un mismo día por el titular de la tarjeta, sin superar el saldo disponible en su cuenta corriente, sólo parece haber incumplimiento contractual del cliente con respecto al Banco o Entidad, que podría sancionarse por éste con la retirada de la tarjeta.

Pero incluso superando el saldo disponible no aparece tampoco la responsabilidad penal derivada de hurto o estafa, si es que nos decidiéramos por la admisión de esta última figura a pesar de la objeción doctrinal reseñada. El cajero entrega la cantidad porque ha sido programado para ello: no hay voluntad contraria de la entidad. Sin embargo, si el titular utilizase una tarjeta anulada o caducada, estaríamos ante un hurto; en grado de tentativa si el cajero retuviese la tarjeta.

Si la extracción es realizada por un tercero con tarjeta perdida o sustraída pueden apreciarse diversas figuras penales. Si la tarjeta fue encontrada y no devuelta, apropiación indebida; si fue sustraída, hurto; si se obtuvo mediante engaño, estafa; en todos los casos por el importe de la tarjeta en sí. Si se la quiere para usarla y devolverla después, estaríamos ante esas mismas infracciones en su modalidad de uso, que son atípicas. También se ha discutido si podría apreciarse el delito de robo con fuerza en las cosas, puesto que la tarjeta cumple el papel de «llave» y las legítimas sustraídas al propietario tienen la consideración de falsas. Pero esa tesis es rechazada por aquellos que consideran que la banda magnética no tiene el carácter corporal de las genuinas llaves.

Otro caso interesante es la utilización de tarjeta falseada o manipulada.- Para algunos podría incluirse entre las falsificaciones de documentos mercantiles del art. 303 C.P.; otros niegan el carácter de documento a la anotación magnética por no ser legible directamente por el ser humano.

MEDIOS COMISIVOS

En el epígrafe anterior hemos clasificado las figuras –todavía no auténticos tipos por no haberse positivado– más frecuentes que podrían constituir la llamada Delincuencia Informática. Veremos aquí las principales conductas que conforman la acción básica en cada una de aquellas figuras.

-Manipulación. Consiste en la supresión o borrado, modificación, ocultación, cambio de lugar de datos o en la introducción de otros falsos, o bien en la alteración de las instrucciones que constituyen el programa. Según el momento en que se produzca estaremos ante una manipulación previa u operada sobre el input o instrucciones internas del programa; simultánea a la ejecución del programa; y posterior a la misma o realizada sobre el output o datos de salida.

The quick brown fox jumps over the lazy dog. Now is the time for all men. Las manipulaciones en las dos primeras fases indicadas son más peligrosas que en la tercera. Y ello porque una vez programadas estas alteracio-

nes pueden perpetuarse durante el tiempo que se desee (no en vano uno de los rasgos del delito informático es su continuidad) e incluso puede programarse la propia autocancelación de la manipulación operada una vez transcurrido determinado plazo lo que borraría cualquier pista de ella.

-Espionaje. Agrupa actividades de obtención no autorizada de datos o programas, o bien de divulgación de los obtenidos legítimamente. Su motivación puede ser fundamentalmente comercial, industrial o militar.

-Sabotaje. Referido a conductas que persiguen la destrucción o incapacitación de los sistemas informáticos o de alguno de sus elementos (hardware y software), con la consiguiente paralización de actividades empresariales o administrativas que ello conlleva.

Tanto el espionaje como el sabotaje son técnicas utilizadas principalmente por organizaciones terroristas en sus atentados contra medios informáticos. Como casos más curiosos recordemos el ya extinto grupo CLORO, Comité para la Liquidación o Conversión de los Ordenadores, que se autoproclamaban trabajadores de la Informática a la que consideraban un instrumento de dominación para el control y represión del pueblo. Otras organizaciones pretendidamente «pacifistas» dirigieron su violencia contra sistemas informáticos al servicio de instalaciones militares como la OTAN, o simplemente civiles, como la central telefónica de Ríos Rosas en Madrid.

COMISION, PERSECUCION Y PREVENCION

Un factor que contribuye en gran medida a la comision de delitos informáticos es el hecho de que la mecanización que supone la informática no se haya compensado con el establecimiento de los oportunos controles informáticos y contables. Estos controles sustituirían a los que antes de dicha mecanización se efectuaban manualmente. Después nos referiremos a la llamada seguridad informática, como vía de prevencion de esta forma delictiva.

Son factores que dificultan la persecución de estos delitos la falta de una legislación específica y la escasa preparación los Cuerpos de Seguridad del Estado en materia informática. Recordemos a este respecto que en EEUU se ha creado recientemente la llamada Policía Informática para la investigación y obtención de pruebas suficientes. El ejemplo nos demuestra cómo el personal investigador ha de reunir conocimientos interdisciplinares en materia infomática, empresarial y jurídico penal.

Además, en la investigación de los delitos informáticos tenemos el «handicap» de que ya la misma averiguación de si el crimen ha sido efectivamente cometido es difícil, mientras que en los tipos clásicos por lo menos este dato suele ser evidente por señales mas o menos patentes, aunque se ignoren otras circunstancias que por ello han de ser objeto de investigación (autoría, móvil, etc).

Pero reunir las pruebas que fundamenten la acusación es sólo el principio del final. Comienza ahora un largo y tortuoso itinerario procesal–penal hasta conseguir una sentencia condenatoria. Baste con pensar que, aun habiendo obtenido, por ejemplo, la cinta que contiene el programa manipulado, será necesario presentar una transcripción impresa de dicho programa, gracias a la intervención de peritos informáticos puesto que ni el notario ni los jueces suelen serlo. Y así en cada trámite en que se exija acreditar la concordancia entre los lenguajes código y fuente del software.

En conclusión, como dice Luis Camacho, experto en seguridad informática, el daño producido por un fraude informático o mejor dicho, el perjuicio, se calcula sumando al importe de lo defraudado, el coste de la investigación, más las ineficacias en el trabajo derivadas de las pérdidas de tiempo y preocupación por el hecho, mas el deterioro de imagen que la publicidad provoca entre los clientes, más el costo de la duda de lo que puede haberse defraudado sin haberse descubierto todavía.

En materia de prevención de esta delincuencia confluyen diversos factores. Uno de ellos es la seguridad de los propios elementos informáticos. Primero se establecieron medidas puramente físicas como servicios de extinción de incendios o sistemas para impedir o detectar el acceso de personas no autorizadas a las instalaciones informáticas.

Más tarde se han comenzado a implantar –todavía en grado insuficiente– medidas de seguridad propiamente informática como controles internos, pistas de auditoría y otras técnicas para evitar la manipulación o sustracción de datos y programas.

Si bien el ideal sería que dichas medidas tuvieran carácter preventivo, disuadiendo de la comisión de estos delitos, en la práctica, por su escasa implantación, muchas veces se adoptan a posteriori de la producción del daño. Finalidad reparatoria tienen las medidas llamadas de «recuperación». Estas pretenden, una vez producida la inutilización en todo o en parte del sistema informático, su reinstalación en un lugar alternativo para la reanudación lo más pronto posible de la actividad empresarial paralizada, minimizando con ello los perjuicios originados.

Otro factor de prevención es el frecuente chequeo del sistema informático para detectar fallos, retrasos, y otras irregularidades, y poderlos subsanar en cuanto antes. De lo contrario se convierten en probables vías de delito.

Pero como en tantas otras cuestiones, en esta de la prevención de la criminalidad informática es preciso combinar el factor técnico con el humano. Por ello junto a las medidas de seguridad antes vistas, es conveniente una buena política de selección y relación con el personal de la empresa de que se trate, y una creciente mentalización de la necesidad de proteger uno de los activos fundamentales en cualquier actividad moderna: los sistemas informáticos.

DERECHO COMPARADO

No puede tenerse una visión con perspectiva de la problemática de la Delincuencia Informática sin tener presente la situacion en los países de nuestro entorno. Tanto la Ley Francesa de 1978, como las Alemanas de 1977 y la de 1986 sobre criminalidad económica establecen un juego de sanciones de diversa naturaleza: penal –multa y privativa de libertad–, administrativa y civil.

Por su parte la Ley Sueca reformada en 1979, contempla supuestos como la creación o explotación de archivos informáticos de datos personales, sin autorización, y sanciones como la declaración de ilegalidad de tales actividades y cierre del banco de datos. También se refiere a la infracción de las instrucciones que la Inspección dicte al conceder las oportunas licencias o a la transacción de datos a otro sistema informático sin las debidas garantías.

TIPICIDAD DE LOS SUPUESTOS DE DELINCUENCIA INFORMATICA

Después de haber examinado la realidad delictiva en el mundo informático hemos de plantearnos si nuestro ordenamiento jurídico está preparado para hacerle frente a dichas situaciones, dotarles de una regulación y resolverlas.

Mas concretamente:

1. ¿Conviene la tipificación de los diversos supuestos de la mal llamada delincuencia informática estudiados? ¿De cuáles?
2. En caso afirmativo ¿podrían englobarse en los tipos penales existentes en nuestro Código o en otras leyes especiales?
3. ¿Es necesario para ello retocar su articulado o incluso crear nuevas figuras?

Para tratar de responder a estos interrogantes hay que partir del principio de intervención mínima según la naturaleza del bien jurídico tutelado, la intensidad del ataque y el contexto social. Pero para que este principio penal cobre verdadero significado, o dicho de otro modo, pueda evitarse una hipertrofia del Derecho Penal, es imprescindible que exista previamente una regulación administrativa de la materia informática.

Es preciso un marco jurídico que defina el ámbito de la actividad cibernética, delimitando los supuestos admitidos de aquellos otros rechazables. Entre estos últimos, sólo aquellos que más radicalmente repugnan a la conciencia social, deben tipificarse. Ese estatuto jurídico administrativo, previo al penal, habría de contener ya medidas de seguridad que fueran eficaces controles con finalidad preventiva de los ilícitos mas graves.

Es preciso, pues, evitar los dos extremos: intervención mínima, sí; pero suficiente. Una vez que se han discernido cuáles son las conductas más mere-

cedoras de sanción penal, debe estudiarse si conforme a la propia técnica penal y a otro principio jurídico básico, el de legalidad, pueden subsumirse en los tipos existentes.

Admitamos que los dos pilares fundamentales en toda disciplina jurídica son la seguridad y la justicia. Veremos cómo el castigo penal de las conductas mas rechazables a través del criterio de la proporcionalidad garantiza la justicia. Fijémonos ahora en el otro pilar: la seguridad jurídica viene representada por el principio de legalidad, que en el campo penal dota de claridad y taxatividad tanto a las conductas prohibidas como a las sanciones impuestas.

También respecto al principio de legalidad penal debe observarse un equilibrio. Por un lado es cierto que una de sus consecuencias lógicas es la prohibición de la analogía contraria al reo, lo cual podría frenar la asimilación de los delitos informáticos a los tipos ya existentes. Pero también es verdad que no se precisa una detalladísima descripción de las acciones típicas, sino que se permite la interpretación extensiva, lo cual facilita la inclusión de las contravenciones informáticas en el Código Penal.

Ocurre además que en multitud de supuestos la intervención de la informática en la comisión del ilícito no altera esencialmente su repercusión lesiva para el perjudicado. Así por ejemplo una falsedad lo seguirá siendo ya se utilice escritura manual, mecanográfica o de otro tipo. Cuando esto ocurra no está justificada la creación de tipos nuevos. Por su parte, sería interesante plantearnos si estas formas de delincuencia se están dejando de detectar y perseguir por motivos ajenos a su actual atipicidad. Pensemos en factores sociológicos como aquella resistencia de la víctima a la publicidad.

La presencia de especificidades en los delitos informáticos como por ejemplo su frecuente carácter continuo, debía resolverse en la Parte General del Código estableciendo un plus punitivo para los delitos cometidos con auxilio o en relación a sistemas informáticos. Además, y aunque ello no sea objeto del presente estudio, esta técnica resultaría muy conveniente respecto de muchas otras materias, como por ejemplo la delincuencia de funcionarios, porque son innumerables los preceptos en que la condición de funcionario se contempla aislada, casuísticamente para matizar determinados supuestos; cuándo sería conveniente que por razones de claridad y economía se regulara globalmente como una circunstancia agravante genérica, con una penalidad especifica.

En conclusión, hoy en día en el Derecho comparado parece existir una dualidad de vías de tipificación de las conductas informáticas: la creación de nuevos tipos y la reinterpretación, incluso teleológica, de los existentes para dar cabida las nuevos supuestos.

La elaboración de tipos específicos o de equivalencia (Alemania, Austria, Portugal) tiene como ventaja la seguridad jurídica y la concreción que supone. Pero junto a ello, el peligro del casuismo que pretendiendo recoger

todos los supuestos pronto implique obsolecencia dado el ritmo del avance tecnológico y la práctica imposibilidad de comprensión de todas las hipótesis. Si no gozan estos nuevos tipos de la suficiente elaboración doctrinal no sólo no resolverán las cuestiones para las que se suponen que fueron creados, sino que contribuirán al surgimiento de nuevos problemas.

La interpretación de los tipos existentes es precisa para la adecuada matización del bien jurídico, el objeto material y las modalidades comisivas, entre otros factores. Con ello se completarían los tipos existentes actualizándolos pero sin crear tipos autónomos. También se mejoraría su técnica corrigiendo cuestiones como la determinación de la pena por el importe del daño y no por el del perjuicio resultante. Todo ello repercutiría en favor de su aplicabilidad a las conductas informáticas.

Lo cierto es que se hace necesaria una reforma de los delitos de daños e incendios en relación no ya sólo a la informática sino a todas las tecnologías de la información y su incidencia en determinados bienes jurídicos dignos de tutela.

Por último y para cerrar el sistema que se propone, el principio de intervención mínima se salvaguarda mediante una política criminal tendente a incriminar sólo las conductas intencionales, excluyendo las culposas y, como es lógico, las debidas a errores técnicos de empleados o fallos de funcionamiento del sistema. Tampoco olvidemos nunca que el Derecho Penal constituye la última ratio, por lo que antes de acudir a él deben agotarse otros recursos, de ahí la conveniencia de coordinar las diferentes vías de protección extrapenal del software: la Propiedad Intelectual e Industrial, en su caso.

EPILOGO

Podemos concluir volviendo a la idea inicial de este trabajo: en los albores del siglo XXI una de las plagas que nos acechan en los países desarrollados son las consecuencias deshumanizantes o indeseables de las nuevas tecnologías. Es preciso adecuar nuestro ordenamiento –en este caso penal– a la situaciones planteadas por la Informática para mitigar esos efectos negativos. Además esa adaptación constituye un proceso contínuo en que por principio el Derecho irá a la zaga de la realidad. Pero por lo menos que el desfase entre aquél y ésta sea el menor posible.

BIBLIOGRAFIA

CAMACHO LOSA, LUIS. «EL Delito informático», Gráficas Cóndor, SA, Madrid, 1987.

CORCOY, MIRENTXU, «Protección penal del sabotaje informático. Especial consideración de los delitos de daños». *La Ley,* 1990, tomo I, págs. 1000 y ss.

CORCOY, MIRENTXU y JOSHI, UJALA, «Delitos contra el patrimonio cometidos por medios informáticos» Revista Jurídica de Cataluña núm. 3.º, 1988. Págs. 133-154.

GONZÁLEZ RUS, JUAN JOSÉ, «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos.» Poder judicial, núm. Especial IX, págs. 39-51.

ROMEO CASABONA, CARLOS MARÍA, «Los delitos de daños en el ámbito informático» Revista de Política Criminal», núm. 43, Madrid, 1991, págs. 91-118.

RUIZ VADILLO, ENRIQUE, «Tratamiento de la delincuencia informática como una de las expresiones de criminalidad económica». Poder Judicial, núm. Especial XI, págs. 53-79.

La criminalidad defraudatoria por medios informáticos en el anteproyecto de Nuevo Código Penal de 1992

M.ª LUZ GUTIÉRREZ FRANCÉS
Departamento de Derecho Público (Area de Derecho Penal)
Universidad de Salamanca
(ESPAÑA)

I. Como la generalidad de los países de nuestro entorno, también España se ha incorporado en las últimas décadas a lo que ya se conoce como *la era de la informática*. El fenómeno de la *computer dependency* hoy se constata con claridad en nuestro país en, prácticamente, todas las manifestaciones del quehacer cotidiano que, en mayor o menor medida, se ven afectadas, dirigidas o controladas por el ordenador –directa o indirectamente–. Es difícil imaginar la actividad de las Administraciones Públicas, o la de sectores como el bancario, el bursátil, el de seguros, transportes o educación... sin la ayuda indispensable de estas, cada vez más sofisticadas y completas, máquinas. Si a ello añadimos el extraordinario incremento de ordenadores personales que hoy ocupan mesas y escritorios privados, podemos decir que las nuevas tecnologías de la información se han instalado de forma irreversible en nuestra sociedad.

Nadie discute que corresponde al ordenamiento jurídico en su conjunto encauzar y disciplinar esta nueva realidad sin limitar el progreso que la informática comporta. Pero, precisamente, el Derecho Penal, por su propia naturaleza como instrumento último de control social, está llamado a conocer, sobre todo, de la informática como factor criminógeno. El Derecho Penal debe enfrentarse a la dimensión pervertida y abusiva de lo que se concibió como

un elemento de progreso, destinado a incrementar casi ilimitadamente las posibilidades del hombre. En efecto, la informática se presenta ante el Derecho Penal con un doble papel: de una parte como *objeto* del delito (tanto en sus componentes físicos como en sus elementos lógicos) y, de otra, como *instrumento* del comportamiento criminal (bien de los delitos clásicos, bien de otros de nuevo cuño).

II. La mayor parte de los ordenamientos penales de modernos han sido objeto, recientemente, de notables reformas con el fin de dar cabida a esta nueva realidad criminal surgida al hilo de las modernas tecnologías de la información. (Sirvan como ejemplo, las reformas portuguesa de 1982, alemana de 1986, japonesa de 1987, o la francesa de 1988 (SIEBER, 1986; GUTIÉRREZ FRANCÉS, 1991a).) Sin embargo, nuestro Código Penal, todavía asentado en el viejo texto de 1848, no se ocupa de dicho tema, ni aun después de las sucesivas reformas de que ha sido objeto en el proceso de transición democrática. En consecuencia, y a falta de alguna previsión específica, los instrumentos jurídico-penales para combatir el *computer crime* no van más allá de los tipos penales tradicionales, cuyas limitaciones han sido largamente reflejadas por la doctrina (ROMEO CASABONA, 1988; GONZÁLEZ RUS, 1986) y de cuyo examen no podemos ocuparnos en este momento con carácter general.

Por lo demás, el estudio de los malogrados textos de 1980 y 1983 revela que la lucha contra la delincuencia informática tampoco constituía uno de los objetivos prioritarios en la actualización del Derecho Penal español que buscaban tales proyectos. (Basta, en tal sentido, recordar la escueta referencia del art. 189 de la PANCP, por citar el último de dichos textos, incardinado entre los atentados contra la intimidad, seguido por el más absoluto olvido en cualquier otra parcela, incluida la de la delincuencia patrimonial y económica.)

III. A comienzos del presente año, ha sido presentado a la opinión pública el Anteproyecto de Nuevo Código Penal de 1992, en breve *Proyecto*, a tenor de lo anunciado recientemente por el Ministro de Justicia. A lo largo de su articulado encontramos, ahora sí, una mayor sensibilidad ante el problema de la delincuencia informática: por primera vez se considera como verdadero problema, que debe ser abordado por un Código Penal moderno. Pero, además, se acaba con la errónea simplificación en que incurrían los proyectos anteriores al estimar como único delito informático posible el atentado «contra la intimidad por medios informáticos». Del texto de 1992 se desprende que no hay una única clase de delitos informáticos, sino que la delincuencia informática es un fenómeno más complejo. Hallamos, así, referencia a la informática como *objeto* de hechos ilícitos (especialmente, atentados contra los elementos lógicos de los sistemas informáticos, en las infracciones de los derechos de la propiedad intelectual, arts. 255 y siguientes) y referencias a la informática como *instrumento* de delitos, creando nuevos

tipos penales tanto en el campo de los delitos contra la intimidad, como en el de los delitos patrimoniales y socioeconómicos.

Esta primera valoración positiva ha de ser, sin embargo, inevitablemente matizada, no sólo por la concreta fórmula adoptada para la tipificación de estas conductas, sino también por la subsistencia de importantes lagunas. (Pensemos, a título de ejemplo, en las falsedades por medios informáticos, el espionaje o el sabotaje informático.) Mas, debido al carácter de la presente intervención, nos detendremos en una parcela concreta, de importancia creciente por su magnitud y efectos, y foco de prioritario interés en otros países aunque, sorprendentemente, con frecuencia sea olvidada en España: nos estamos refiriendo a las defraudaciones por medios o procedimientos informáticos (el fraude informático o *computer fraud*).

IV. A las defraudaciones patrimoniales por medios informáticos destina el Anteproyecto de 1992 dos preceptos:

– El primero, hace referencia a las conductas de utilización ilícita o abusiva de tarjetas electromagnéticas, que se resuelven como robos con fuerza por virtud del art. 238 in fine, donde se establece: *A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.*

– El segundo de ellos, pero primero en importancia a nuestro juicio, es el art. 248.2, donde se tipifica, entre las defraudaciones y a continuación del tipo básico de estafa, la estafa mediante ordenador, en los siguientes términos: (248.2) *También cometen estafa los que, con ánimo de lucro, realizan una manipulación informática que interfiera el resultado de un procesamiento o transmisión informática de datos y así ocasionen un perjuicio a otro.*

V. Primer foco de atención, por tanto: el art. 238 *in fine*. Si prospera este precepto en un futuro Código Penal, todas las conductas de utilización ilícita de tarjetas con banda magnética, perdidas por su titular o substraídas al mismo, para la obtención de dinero de cajeros automáticos, serán subsumibles en el tipo de robo con fuerza (art. 237 del Anteproyecto). Ciertamente, no era desconocida en nuestro panorama jurídico la solución por la que ha optado la Comisión redactora del Anteproyecto en este artículo. En la misma línea ya se habían pronunciado parte de nuestra doctrina, la propia Fiscalía General del Estado y, también, nuestros tribunales (BACIGALUPO ZAPATER, 1989; FISCALÍA GENERAL DEL ESTADO, 1989).

Sin embargo, como ya hemos manifestado en otro lugar (GUTIÉRREZ FRANCÉS, 1991b), a nuestro juicio la fórmula adoptada no es, del todo, incontestable. No vamos a cuestionar lo que aportaría, en términos de seguridad jurídica, la contemplación de estas conductas por el Derecho positivo, cualquiera que sea su ubicación sistemática. En estos momentos, se demanda con urgencia la unificación del tratamiento jurisprudencial de, prácticamente, idénticos hechos, unificación que sólo puede llegar de la mano del Derecho

positivo. Mas, admitido dicho extremo, dirigimos nuestra crítica a la reconducción de comportamientos con una evidente dinámica comisiva defraudatoria, a la sede de los delitos de apoderamiento material. El papel de una tarjeta electromagnética en un atentado patrimonial no siempre es asimilable al que desempeña una llave en los delitos de robo con fuerza.

Pensemos, a modo de ejemplo, en los siguientes supuestos:

– A sustrae a B la tarjeta magnética que le posibilita la apertura de su caja fuerte, la abre y se apodera de los objetos de valor que encuentra en la misma.

– A sustrae a B su tarjeta con banda magnética, encontrando junto a ella el número de identificación personal que le permite realizar diversas operaciones bancarias desde los cajeros automáticos de determinada entidad. Valiéndose de dicha tarjeta, y utilizando el referido número, A obtiene una fuerte suma de dinero de la cuenta corriente de B.

A pesar del paralelismo entre ambos supuestos, entendemos que existe una notable diferencia en la dinámica comisiva desarrollada. La primera, propia de los delitos de apoderamiento (cuando A sustrae y utiliza la tarjeta magnética ajena está superando el obstáculo que ha colocado el propietario para proteger su propiedad. Accede, así, a la cosa de la que se apodera *sin* o *contra* la voluntad del propietario.) En el segundo supuesto, en cambio, se aprecia la dinámica comisiva propia de las defraudaciones (cuando A utiliza la tarjeta magnética de B y su número de identificación personal, está engañando al banco. Se está presentando ante la entidad bancaria –a través del ordenador que la misma ha preparado para que realice determinadas operaciones según un programa– como el verdadero titular de la cuenta corriente a la que ha ganado acceso, titular que es el único legitimado para detraer fondos de dicha cuenta. Y el banco, siempre a través de la máquina, realiza la disposición patrimonial con la creencia errónea de que la efectúa al titular. Es decir, el dinero no se obtiene *contra* la voluntad del banco, sino con un consentimiento viciado por el error.) (DE LA MATA, 1989).

Así pues, el tratamiento indiferenciado de todas las conductas de utilización ilícita o abusiva de tarjetas magnéticas y su reconducción al tipo de robo con fuerza nos parece criticable.

VI. La siguiente referencia objeto de nuestro análisis: el nuevo tipo de estafa informática del art. 248.2.

La incorporación al Código Penal de una figura de estafa mediante computadora, en la línea de la *Computerbetrug* del Código alemán, también había sido demandada por la doctrina en nuestro panorama jurídico (CORCOY, JOSHI, 1988), y el Anteproyecto de 1992 se ha hecho eco de esta demanda. El planteamiento que subyace a la misma parece claro: se parte de una reducción del complejo fenómeno de los fraudes informáticos a las defraudaciones *patrimoniales* por medio de computadoras (fraude informático como fraude

estrictamente patrimonial por medios informáticos). Tras esta simplificación inicial, se recorren los diversos tipos penales clásicos protectores del patrimonio en busca de un posible ropaje jurídico para estos comportamientos. Se comprueba la imposibilidad de aplicar los tipos existentes sin agredir al principio de legalidad penal y se concluye proponiendo la creación de una nueva figura. Pero, ¿qué figura ha de ser? Como quiera que el delito de estafa es el que revela una peculiar vocación para la represión de las defraudaciones patrimoniales por medios informáticos, se recomienda que la figura de nueva creación sea, precisamente, una estafa especial, un delito paralelo al actual del art. 528 del Código Penal, donde se superen los obstáculos que impiden la aplicación de éste.

De aquí se deduce que el art. 248.2 del Anteproyecto respondería a la necesidad de cubrir una laguna legal detectada en el Derecho vigente en orden a la represión de los fraudes informáticos. (Parece intuirse que estas conductas fraudulentas no constituirían estafa –al menos, muchas de ellas–, de no existir el art. 248.2.) No obstante, al margen del mayor o menor acierto en la formación técnica del referido artículo, el interrogante que surge es el siguiente: ¿en qué medida puede servir esta regulación para la consecución del ambicioso objetivo perseguido?

Para nosotros ya resulta cuestionable el punto de partida, esto es, la delimitación inicial de la categoría de fraude informático. El complejo y heterogéneo mundo de la criminalidad defraudatoria por medios informáticos no puede quedar reducido, por razón del bien jurídico afectado, a los atentados *contra el patrimonio*, en un sentido microsocial individualista.

El fraude informático, hoy por hoy en España, no es una categoría de Derecho positivo, pero tampoco creemos que deba aspirar a serlo como unidad –debido a su contenido heterogéneo, de imposible reconducción a una única figura penal–. En la categoría del fraude informático o defraudaciones mediante ordenador tienen cabida todos los comportamientos de *manipulación, abuso o interferencia en el funcionamiento de un sistema de tratamiento automatizado de datos* (nótese la primacía del componente intelectual subrepticio, caracterizador de las defraudaciones, como motor de la acción), con *intención maliciosa de procurarse un provecho* (dimensión subjetiva, concreción del *animus decipiendi*, también consustancial a lo defraudatorio), *para producir un perjuicio económico* (no necesariamente patrimonial en sentido individualista).

Como se observará, aquí preferimos partir de una noción amplia de fraude informático de caracter funcional, que reúna en sí comportamientos de la criminalidad defraudatoria que atentan contra bienes o intereses diversos, aunque sean siempre de contenido económico. (Mediante manipulaciones fraudulentas de elementos informáticos pueden lesionarse intereses patrimoniales *stricto sensu*, pero también se puede afectar, por ejemplo, al sistema de cotizaciones bursátiles, al sistema crediticio, a la Hacienda Pública en su

dimensión de gasto, a los intereses de los accionistas o de los consumidores, etc.) Y construir una categoría de fraude informático contemplando sólo su dimensión patrimonialista es un planteamieno carente de toda perspectiva de futuro, al sacrificar una importante parcela de la criminalidad informática fraudulenta en relación con intereses valiosos de carácter macrosocial. Una noción de fraude informático, especialmente en el actual momento de reforma penal, no puede construirse utilizando como única plantilla el delito de estafa, y cerrando las puertas a conductas fraudulentas propias de la delincuencia socioeconómica, terreno donde es previsible que las nuevas tecnologías de la información se conviertan en el instrumento idóneo. Las carencias del Derecho positivo español en materia de criminalidad económica no deben suponer un lastre en la elaboración de una propuesta de *lege ferenda.*

El entendimiento de las defraudaciones mediante computadoras en un sentido tan amplio conduce, indefectiblemente, a la siguiente conclusión: en el mejor de los casos, el tipo propuesto por el art. 248.2 del Anteproyecto sólo servirá para reprimir una dimensión de los fraudes informáticos: los que atenten contra el patrimonio como bien jurídico individual microsocial, mostrándose ineficaz frente a manipulaciones informáticas fraudulentas que, sin provocar un perjuicio patrimonial constatable y cuantificable, afecten a otra suerte de intereses económicos de carácter colectivo. (En este sentido, conviene recordar que el Anteproyecto de 1992 no vuelve a referirse a manipulaciones informáticas fraudulentas en la compleja y controvertida regulación de delitos socioeconómicos del Título XII del Libro II. Sin embargo, esto no implica que deban resultar impunes los delitos socioeconómicos realizados por medio de manipulaciones informáticas fraudulentas, cuestión que depende del titulado de tales delitos y de la concreta regulación típica de los mismos.)

En punto a la significación que para nosotros tiene, o debiera tener, el mencionado art. 248.2 del texto de 1992, también diferimos del parecer dominante: su misión, a nuestro juicio, no es tanto la de cubrir una laguna legal, cuanto aclarar, por vía de interpretación auténtica, lo que ya se hallaba incluido en el tipo básico de la estafa. Y, si bien la solución implica un considerable avance en términos de seguridad jurídica, tampoco debe ser magnificada. Las estafas realizadas por medios o procedimientos informáticos (fraudes *patrimoniales* informáticos) pueden ser reprimidas hoy en nuestro Derecho por el tipo del art. 528 vigente, se actúe, o no, con sistemas informáticos total o parcialmente automatizados, como ya hemos defendido en otro lugar. Mas, el reconocer a la estafa alguna virtualidad en este terreno (particularmente, cuando los fraudes se efectúan sobre sistemas informáticos total o parcialmente automatizados), se asienta en dos presupuestos: uno, vinculado a los propios ordenadores y a su función instrumental, y otro, referente a la interpretación del tipo de estafa.

– Por obvio que parezca, lo primero que se precisa es un correcto entendimiento del papel que los ordenadores desempeñan en la vida moderna.

Cualquiera que sea su complejidad y grado de sofisticación, los ordenadores son sólo máquinas al servicio del hombre, que el hombre prepara y dispone para que ejecuten, en concreto, órdenes determinadas. Y, en un comportamiento fraudulento como los que analizamos, sólo serán *instrumento*, pero nunca *víctima o sujeto de la acción*. Hay que desterrar expresiones que conducen a equívoco y tan repetidas como «engaño a una máquina», (a lo sumo, se engaña a alguien utilizando como instrumento la máquina-ordenador), o bien, «ordenador engañado que realiza un acto de disposición» (la máquina sólo *ejecutará*, en su caso, el traspaso patrimonial ordenado y dispuesto por quien ha efectuado, con la programación, el acto de disposición), etc.

– Se precisa, además, una determinada interpretación del tipo de estafa, dentro de las exigencias del principio de legalidad, pero más acorde con el modelo actual de relaciones socioeconómicas. De este giro en la comprensión de la estafa depende la tipicidad o atipicidad de las conductas de fraude informático. Pero, también y sobre todo, la suerte de buena parte de las más modernas manifestaciones de la criminalidad defraudatoria, a cuya cobertura miraba la reforma de este delito en 1983. La reinterpretación del art. 528 que apuntamos afecta esencialmente al tipo objetivo en los puntos que resumimos:

. Respecto al *engaño* típico, es imprescindible aceptar que el falseamiento de la realidad que el engaño implica no comporta, necesariamente, una *relación directa y personal* entre dos seres humanos, emisor y receptor. Hay que huir, pues, de tal exigencia de inmediatez no consustancial al engaño, sino deducida por vía de interpretación y sólo comprensible en otro momento histórico, en el cual dicha nota caracterizaba las normales relaciones del tráfico jurídico.

Por lo demás, en tanto se siga negando –en Derecho penal, que no en otras ramas del ordenamiento– la posibilidad de engañar a una persona jurídica, o a cualquier persona, física o jurídica, cuando actúa en el tráfico jurídico con el auxilio de las altas tecnologías de la información (postura que no compartimos), la figura de la estafa quedará vedada a la mayoría de las nuevas formas defraudatorias, incluidas las defraudaciones mediante ordenador.

. Respecto al papel del *error* en la estafa, con anterioridad, hemos mostrado nuestra preferencia por la tesis –minoritaria– que le niega su condición de elemento autónomo en este delito, circunscribiendo su función a la delimitación restrictiva del engaño típico (GUTIERREZ FRANCES, 1991c). Y, no obstante, entendemos que una lectura moderna y actualizada del tipo de estafa, adecuada a la nueva realidad criminal a la que debe enfrentarse, no precisa llegar a tal solución. Basta, pero es necesario, abandonar la *concepción psicológica* del error (estado psicológico de la *persona humana* consistente en una falsa representación mental de la realidad). Si el ordenamiento jurídico admite sin reservas, por ejemplo, que una persona jurídica puede *consentir* en el

tráfico jurídico con un *consentimiento viciado por error*, ¿por qué no puede admitirlo el Derecho penal?

Desde luego, si para apreciar estafa continúa exigiéndose la producción directa de un estado psíquico de error en una persona –física–, víctima del engaño, la virtualidad de tal figura quedará, prácticamente, reducida al círculo de los timos clásicos, y será inoperante ante las nuevas defraudaciones.

. En lo que concierne al *acto de disposición patrimonial*, también sería precisa una reinterpretación –consecuencia natural de un entendimiento distinto del engaño y del error–, asumiendo, con el resto del ordenamiento jurídico, que se pueden realizar disposiciones patrimoniales con el auxilio de una máquina y que la *colaboración en el traspaso patrimonial lesivo* que este elemento implica puede predicarse, también, de las personas físicas, bien actúen personalmente, bien, a su vez, mediante máquinas. La escisión temporal entre el momento volitivo y la concreta ejecución del acto de disposición no debe inducir a confusión, pues el dominio de la disposición no corresponde al ordenador –que sólo materializa las órdenes que se le han introducido–, sino al que prepara los equipos informáticos y los programas para operar.

VII. En suma, la formulación actual del tipo de estafa en el Derecho español no imposibilita su aplicación a las defraudaciones informáticas, siempre, claro está, que produzcan una lesión patrimonial cuantificable e identificable. No obstante, esto requiere una interpretación del art. 528 que hoy es minoritaria en doctrina y jurisprudencia, haciendo aconsejable alguna regulación por los riesgos evidentes que plantea en términos de seguridad jurídica. Desde esta perspectiva, consideramos positiva la incorporación de una figura como la del art. 248.2 del Anteproyecto, sin más significación que la ya indicada: una aclaración, vía auténtica, de la extensión del tipo de estafa –también aplicable a las estafas realizadas con ordenador–.

En todo caso, dentro de un proyecto tan ambicioso como un nuevo Código Penal, la represión del fraude informático no puede quedar reducida a una solución tan limitada. La lucha eficaz contra esta nueva forma de delincuencia se nos antoja demasiado vinculada a la suerte que corran los llamados delitos socioeconómicos. Y todo parece indicar que, en esta materia, el Anteproyecto deja demasiadas incógnitas.

Finalmente, tenemos que denunciar olvidos apreciables en el texto de 1992, en relación con otras manifestaciones de la delincuencia informática que, eventualmente, pueden estar relacionadas con los fraudes informáticos, como el espionaje o el sabotaje informáticos, las falsedades por medios informáticos, o como las conductas de interferencia y uso ilícito de los sistemas informatizados (*hacking*). En la mayoría de los ordenamientos penales en los que se ha abordado la regulación de los delitos informáticos (así en el Derecho alemán, en el Derecho francés, o en los Estados Unidos de América, por

citar algunos ejemplos) estos hechos han sido tipificados. Sería deseable que nuestro legislador procediese a una regulación más cuidadosa y meditada de esta materia y, como quiera que aún está a tiempo, procurase una comprensión más acabada del complejo fenómeno de la criminalidad informática.

BIBLIOGRAFIA

BACIGALUPO ZAPATER, E., «Utilización abusiva de cajeros automáticos por terceros no autorizados», Poder Judicial, número especial IX (Nuevas formas de delincuencia), 1989, pp. 85 y ss.

CORCOY, M., JOSHI, U., «Delitos contra el patrimonio cometidos por medios informáticos», Revista Jurídica de Cataluña, 3, 1988, pp. 687 y ss.

DE LA MATA, N. J., «Utilización abusiva de cajeros automáticos: apropiación de dinero mediante tarjeta sustraída a su titular». Poder Judicial, número especial IX (Nuevas formas de delincuencia), 1989, pp. 151 y ss.

FISCALÍA GENERAL DEL ESTADO, Memoria elevada al Gobierno de S. M., Madrid, 1989, pp. 521.

GONZÁLEZ RUS, J. J., «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», Revista de la Facultad de Derecho de la Universidad Complutense de Madrid, 6 (Monográfico sobre informática), 1986, passim.

GUTIÉRREZ FRANCÉS, M. L., Fraude informático y estafa, Madrid, Ministerio de Justicia, 1991a, pp. 117 y ss.

GUTIÉRREZ FRANCÉS, M. L., Fraude informático y estafa, Madrid, Ministerio de Justicia, 1991b, pp. 474 y ss.

GUTIÉRREZ FRANCÉS, M. L., Fraude informático y estafa, Madrid, Ministerio de Justicia, 1991c, pp. 284 y ss.

ROMEO CASABONA, C. M., Poder informático y seguridad jurídica, Madrid, Fundesco, 1988a, pp. 51 y ss.

SIEBER, U., The International Handbook on Computer Crime, Chichester, John Wiley and Sons, 1986, passim.

La criminalidad informática: situación de lege data y lege ferenda en CHILE

RENATO JAVIER JIJENA LEIVA
Profesor de Informática y Derecho. Escuela de Derecho de la Univ. Católica de Valparaíso
(CHILE)

I. La **informática**, que con sus múltiples beneficios revoluciona el devenir histórico de nuestras sociedades, eventualmente puede ser usada con fines delictuales. El hecho de estudiar las implicancias de la informática bajo el prisma del Derecho Penal es, por cierto, una tarea novedosa, que abordamos por considerar que **debido a los radicales cambios que ella ocasiona los nuevos delitos no pueden ser analizados solamente con las categorías tradicionales de la criminología**. Ante las interrogantes de si es necesaria la creación de nuevas formas penales que salgan al paso de posibles extralimitaciones en el uso de la informática, o de si estamos ante un fenómeno tecnológico que requiera la intervención del «ius puniendi» del Estado, la respuesta es, a no dudar, afirmativa. Porque la tecnología computacional, no obstante lo trascendente que ha sido y seguirá siendo para las sociedades modernas, **va camino de convertirse en una variante cada vez más presente en los delitos**, situación que se agrava por cuanto los tipos penales que actualmente existen no subsumen, porque no pueden hacerlo, los hechos ilícitos realizados por medio del computador o en contra de un sistema de tratamiento automatizado de información.

II. Hay quienes estiman que la problemática de los delitos informáticos, sea considerando a la computación sólo como un específico medio de comisión o como el objeto directo de un ilícito informático, ...no constituye un factor criminológico que requiere de la elaboración de tipologías y regula-

ciones específicas. Por cierto que los ilícitos y los abusos informáticos en cierta forma han sorprendido a los penalistas, situación que en parte se debe a que el Derecho Penal anterior al desarrollo de la informática no podía precaver sus implicancias criminales y, además, a que por ser novedoso el tratamiento de esta temática, ella se caracteriza por una notable falta de precisión. En nuestra opinión, tanto para ilustrar a los iuspenalistas como para encontrar la necesaria claridad conceptual, no basta con «aggiornar» esta rama del derecho: Es necesario investigar y desarrollar un Derecho Penal de la Informática.

Consideramos que es insuficiente el pretender que los tipos tradicionales contenidos en la mayoría de los Códigos Penales contemporáneos sean capaces de brindar la protección necesaria. Esto no significa desconocer que algunos de los delitos –sobre todo patrimoniales– pueden ser perpetrados mediante computadores (los que pasan a ser específicas herramientas de comisión). No obstante, por la complejidad del medio informático, por las posibilidades que éste otorga para desarrollar nuevas figuras delictivas o perfeccionar las existentes, por las nuevas modalidades de comisión y porque la legislación penal vigente no puede contemplar todos los posibles delitos informáticos, ...**creemos que es imprescindible tipificar una figura específica, por cierto que sin reformar el Código del ramo** (sostenemos la tesis de que deben consagrarse en leyes específicas que regulen el uso de la informática). La necesidad se basa fundamentalmente en el principio de la tipicidad, una manifestación en materia penal del principio constitucional de legalidad, en cuya virtud no puede haber un delito y no puede asignarse una pena sin que previamente una ley lo haya establecido.

III. El delito informático no ha sido objeto de una elaboración conceptual suficientemente perfilada y, en Chile –en general en los países en que el sistema jurídico es legalista– no basta pretender descansar en la labor creadora de la Jurisprudencia, como ocurre en los países anglosajones. Por la falta de tradición jurídica de la temática en comento, una de las principales trabas para la confección de un tipo legal específico es lo difícil que resulta encontrar una definición «standard», que sea comprensiva de todas las circunstancias que involucra la criminalidad informática. Puede definirse como **toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma** (delito informático propiamente tal).

De la definición surge una primera clasificación. Se llaman delitos **computacionales** a **aquellos** hipótesis en que, tratándose de delitos subsumibles por los tipos tradicionales, la informática es solamente una específica herramienta de comisión que actúa como agravante de la penalidad asignada (V.gr. hurto de valores vía transferencia electrónica de fondos). Son delitos **específicamente informáticos** (V.gr. virus, bombas lógicas o destrucción de infor-

mación, acceso ilícito a los datos, etc.), aquellos en que el objeto material y el bien jurídico afectado es la información tratada automatizadamente. Téngase presente que al tipificarse un delito informático lo que se busca es tutelar el contenido de información (soporte lógico) de un sistema de tratamiento automatizado de la misma y no el soporte físico-tecnológico en que aquel se almacena; así, la apropiación (hurto o robo) o la destrucción (daños o incendio) de un P.C. (Personal Computer), de un disco duro, de un diskette o de una cinta magnética..., independientemente del contenido informacional, son hipótesis perfectamente captables por los tipos del Derecho Penal común.

El concepto de delito informático se ha caracterizado como una acción delictiva en la cual el ordenador es instrumento u objeto del ilícito, definición amplia pero apropiada para acercarse al problema: En algunos casos el computador es objeto del delito; en otros un medio para cometer un hecho delictivo. Se distingue por ende entre los delitos **con medios informáticos**, para aludir a los casos en que la computación es la herramienta o el medio de comisión del hecho punible y los delitos **contra medios informáticos**, cuando pensamos en la lesión del contenido de información de un sistema que será objeto de tratamiento automatizado, o que está siendo procesado o que ya ha sido almacenado y en cómo los datos o programas pueden verse afectados por el delito. Generalmente los delitos contra son cometidos con medios informáticos, pero puede ocurrir que los instrumentos para perpetrarlos no estén vinculados a la tecnología computacional, como cuando acercándole un imán se destruye la información de un disco o de una cinta magnética.

La muy reciente doctrina jurídica que aborda la criminalidad informática distingue básica y sistemáticamente –para analizar los delitos que pueden cometerse en un sistema de tratamiento automatizado de información, sea contra el «hardware» o soporte tecnológico, sea contra el «software» o soporte lógico (programas y datos)– cuatro modalidades: El **«fraude informático»** para aludir a las manipulaciones de programas y datos almacenados, al ingresarlos o al procesarlos; el **«sabotaje informático»** o destrucción o inutilización, sea del equipo o «hardware», sea de los datos o programas (vía programas virus, bombas lógicas, etc.); el **«espionaje informático»** u obtención ilícita de información almacenada –sin autorización– y el **«hurto de horas de computador»**, que consiste en el provecho personal o de terceros que consigue el delincuente al operarlo, sin mediar autorización, fuera del tiempo o del propósito a que está destinado.

IV. Concluímos que el derecho penal debe amparar los contenidos informativos de un sistema, **la información** misma, sin apellidos. Y al no calificarla en un principio **la concebimos genéricamente y proyectable a los restantes bienes jurídicos afectados**: Si la información es nominativa se atenta contra la **intimidad**; de ser económica contra la **propiedad** o el patrimonio; y de ser estratégica o relacionada con la seguridad o la soberanía de un Estado contra lo que hemos denominado la **intimidad nacional**. Pero

además, creemos que la información –el conjunto organizado de datos o el soporte lógico informático– **constituye el objeto material** de un delito informático, no obstante ser intangible e incorporal, con lo cual, retomando la configuración genérica que recién formulamos y para mantener coherencia con la misma, planteamos un doble alcance para la información: **Sería un bien jurídico esencial para la sociedad y se vería afectada directa y materialmente por un ilícito informático**. Por cierto que no sabemos de alguien que comparta este desdoblamiento.

V. Para poner de manifiesto la insuficiencia de los tipos tradicionales, consideremos **el delito de hurto**, que es de apropiación (porque hay un desplazamiento patrimonial) y cometido por medios materiales (con una actividad dirigida a la apropiación de la cosa). Sobre la base del artículo 432 del Código chileno del ramo (la situación es igual en España), el hurto se define como la apropiación de hecho de una cosa mueble ajena, sin la voluntad de su dueño, con ánimo de lucrarse y sin que concurran violencia o intimidación en las personas. Para los efectos de este delito **sólo son cosas** (objeto material) **las corporales que permitan su apoderamiento físico, excluyéndose las inmateriales**, como los derechos, que para el Código Civil también son cosas. Así, este tipo no alcanza a comprender, por ejemplo, la sustracción de datos, por la exigencia de que la apropiación debe recaer sobre una cosa mueble ajena y porque la información es un bien mueble, pero inmaterial, incorporal o intangible, cualquiera que sea el soporte físico informático que la contenga.

Porque no es subsumible en el tipo del Código Penal, el hurto de «software» o del soporte lógico informático requiere de la tipificación de un delito informático. Se trata de contenidos de información, impulsos eléctricos, «bits» (programas y también datos), cuyo valor excede ampliamente al del soporte físico (diskette, cinta) que los contiene.

VI. La única situación actualmente regulada en Chile es el problema de la **«piratería de programas computacionales»**, en virtud de sucesivas modificaciones introducidas a la ley 17.336, sobre propiedad intelectual. Pero esta modalidad de copia ilegal de software **no constituye un delito informático sino que se trata de un delito contra la propiedad intelectual**: El artículo 80, letra b, sanciona a quien intervenga, con ánimo de lucro, en la reproducción, distribución al público o introducción al país y a los que adquieran o tengan con fines de venta programas computacionales.

El Ministerio de Justicia del pasado gobierno, entre 1986 y 1988, elaboró –incurriendo en serios errores de fondo, que ahora no cabe desarrollar– un Proyecto de Legislación Informática, cuerpo prelegislativo en el que se tipificó un delito informático específico. Para el análisis del texto normativo en comento, puede considerarse una cierta evolución, a la cual dedicamos el

Capítulo V de nuestro libro «Chile, la protección penal de la intimidad y el delito informático».

A nuestro parecer, dos son sus **contenidos fundamentales: la regulación del tratamiento automatizado de información nominativa y la criminalidad informática.** El artículo 1.º se extiende en la descripción de los datos amparados por el proyecto (ámbito de aplicación), aludiendo específicamente a los datos personales, los de familia y los concernientes a los derechos y deberes garantizados por la Constitución Política. Un informe técnico señaló que el proyecto en estudio se refería a la recolección y difusión informática de datos personales, es decir, datos que permiten la identificación del sujeto al que se refieren, quedando los demás al margen de esta legislación. Despejando toda duda interpretativa, consignaba que era la aplicación de la informática la que hacía necesaria la promulgación de una ley que cautelara y protegiera la vida privada de las personas. Sin lugar a dudas que **el mayor logro lo constituyó el haber insertado en una ley de protección de datos un específico tipo de delito informático**, en que el objeto material afectado es el soporte lógico del sistema, ...la información (datos y, necesariamente, los programas) destinada a ser procesada, durante su procesamiento o contenida en un sistema computacional.

El **artículo 30** supone la comisión con medios informáticos de los delitos contemplados en la legislación penal, agravándose su penalidad (agravante especial). Esta figura, que tácita o indirectamente vino a modificar el CP., estimamos que se presenta como un complemento importante al delito tipificado en el artículo 31, por cuanto evita posibles dudas o vacíos de interpretación y amplía la protección penal de los bienes jurídicos que eventualmente pueden verse afectados por la criminalidad informática.

El **artículo 31** es el más importante, por cuanto tipifica en forma amplia un delito específico o propiamente informático, señalando: «Comete delito informático el que maliciosamente y sin derecho o autorización realice cualquier acto con la finalidad de obtener acceso, de apoderarse, de destruir o inutilizar, transformar o desfigurar la información contenida o destinada a ser procesada, en todo o en parte, en un sistema automatizado de tratamiento de la misma; o con la finalidad de impedir u obstaculizar el normal procesamiento de los datos contenidos en un sistema automatizado; o con la finalidad de revelar o transmitir indebidamente información. El culpable de este delito será sancionado con la pena de presidio menor en su grado medio a presidio mayor en su grado mínimo, según la extensión o cuantía del daño causado».

– Se considera en el tipo que tres pueden ser los fines posibles del autor del delito. Analizándolos, claramente se observa cómo se ampararon los datos en los diferentes estados en que pueden encontrarse: a) La información destinada a ser procesada; b) Durante su «normal procesamiento», y c) La información contenida en un sistema informático.

El **artículo 32** introduce otro tipo penal, el que consideramos bastante

cuestionable. La norma señala: «Igualmente comete delito informático el que organice o utilice un sistema de tratamiento automatizado de información con un propósito ilícito. El culpable de este delito sufrirá las penas del artículo 293 del CP».

– Este artículo derechamente es atacable de inconstitucionalidad por falta de tipicidad, en consideración a lo que dispone el artículo 19 Nº3, inciso 8º de la Constitución Política de 1980. En efecto, allí se establece que la Constitución asegura a todas las personas, Nº3: «La igual protección de la ley en el ejercicio de sus derechos». En materia penal esta igualdad está desarrollada en los incisos 7º y 8º, señalando el segundo que «ninguna ley podrá establecer penas sin que la conducta que se sanciona esté expresamente descrita en ella». Precisamente, el artículo 32 del proyecto no describe expresamente la conducta en él sancionada, cuando utiliza como parte de la hipótesis de hecho, la expresión **«con un propósito ilícito»**.

VII. El cuerpo prelegislativo en comento ha sido recogido por los actuales parlamentarios chilenos, en una moción de ley que debiera ser colocada en tabla durante el presente año, para su análisis en la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados. Por lo mismo, para terminar y en un plano de «lege ferenda» o de «ideas sobre cómo legislar», queremos formular los siguientes alcances que deberán considerarse:

– Frente a conductas en que dolosamente se atente contra el contenido de información de un sistema informático –no sólo nominativo–, la tutela requerida pasa por la tipificación de hipótesis de **delitos informáticos**, también insertos en una ley de protección de datos.

– Valorativamente, la intimidad, la información nominativa, es el más relevante de los bienes jurídicos afectados por la criminalidad informática. En Chile, algunos abogados que incluso participaron en la revisión del proyecto en comento, descartan la tutela penal de la intimidad –vía delitos informáticos– y consideran de mayor relevancia al patrimonio, ...porque los perjuicios económicos suelen ser considerables. No obstante ser importante la criminalidad patrimonial informática, se trata de una opción que no podemos, por formación y convicción, compartir. Cuando se viola computacionalmente una garantía de rango constitucional, un derecho primordial para la dignidad, libertad y seguridad de las personas, deben poder aplicarse las sanciones más drásticas que contempla un ordenamiento jurídico, es decir, las penales, que implican privación de libertad; y éstas deben tipificarse.

– **Tampoco existe discusión doctrinaria alguna sobre si los atentados contra la intimidad deben ser ilícitos civiles o penales**. Hay quienes señalan que las conductas «negligentes o culposas» debieran ser sancionadas en sede de responsabilidad civil, descartándose la tipificación de cuasidelitos informáticos. Pero no sabemos de nadie, después de seis años de investiga-

ción en Chile y en el extranjero, que afirme que las conductas «dolosas» no deban sancionarse penalmente: para efectos del resarcimiento por la intromisión dolosa en la intimidad de una persona, se requiere que el hecho sea constitutivo de delito; así, «la configuración del delito informático como una figura punible distinta, es la única solución que permitirá resolver el problema desde el punto de vista del hecho ilícito».

Aspectos legales de los virus informáticos

JULIO TÉLLEZ VALDÉS
Doctor en Informática Jurídica y Derecho de la Informática por la Universidad de Montpellier I
Investigador en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.
(MEXICO)

SUMARIO

I. GENERALIDADES
II. ORIGEN DEL VIRUS
III. CAUSAS
IV. TIPOS DE VIRUS
V. EFECTOS
VI. MEDIDAS PREVENTIVAS
VII. MEDIDAS CORRECTIVAS
VIII. SEGURIDAD EN LOS CENTROS DE COMPUTO
IX. ELEMENTOS JURIDICOS
X. CONSIDERACIONES FINALES

I. GENERALIDADES

El virus informático, aunque difícil de conceptualizar dada su misma naturaleza técnica a pesar de ser una expresión con inevitables recubrimientos científicos derivados de la acepción «virus», se ha considerado como un pro-

grama que puede infectar a otros, modificándolos para incluirles una copia ejecutable de sí mismo o cambiar parte del código.

El virus puede extenderse cuando el usuario hace uso de el programa contagiado, infectando a otros discos y programas.

La mayoría de los virus no dejan señales externas de su presencia despues de infectar; un programa infectado puede operar normalmente por cuatro meses o hasta ocho años sin dar señal de alguna infección.

Durante este tiempo el virus se reproduce calladamente en otros programas del sistema operativo y en diskettes insertados en la computadora. Después de un período de reproducción el virus se activa, entonces se manifiesta el disturbio que tiene el sistema, ya sea con mensajes, con la aparicion de figuras flotantes, o bien, puede causar una parcial o total destrucción de información almacenada.

Estos virus, en la mayoría de las ocasiones se introducen en las computadoras con motivo del uso indebido de algún equipo o programa, provocando desde la interrupción de las sesiones de trabajo y la pérdida de datos o archivos en los medios de almacenamiento de información, hasta daños al propio sistema. Son «programas» reducidos que en pocas líneas contienen instrucciones, parámetros, contadores de tiempo o del número de copias, mensajes, etc.; casi nunca incluyen el nombre del autor, ni el registro ni la fecha, reproduciéndose a sí mismos y tomando el control o modificando otros programas.

La Computer Virus Industry Association, integrada por compañías y programadores que desarrollan programas destinados a la prevención, detección y erradicación de virus, ha agrupado a estos en tres clases distintas: infectores del área de carga inicial (boot infectors), infectores del sistema e infectores de programas ejecutables (extensión com o exe):

a) Infectores de carga inicial: infectan los diskettes o el disco duro, alojandose inmediatamente en el área de carga, o sea, en el sector 0. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo. Aún en caso de reinicialización del ordenador, el virus permanece en el sistema e infecta el disco inmediatamente si este no esta protegido contra escritura.

b) Infectores del sistema: se introducen en los programas del sistema, por ejemplo, el command.Com y otros que se alojan como residentes en memoria. Los comandos del dos, como COPY, DIR o ERASE, son programas que se introducen en la memoria al cargar el sistema operativo y es asi como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver su directorio.

c) Infectores de programas ejecutables: estos son los virus más peligrosos ya que se diseminan fácilmente hacia cualquier programa como es el caso de las hojas de cálculo, juegos, procesadores de textos, etc. La infección se produce al ejecutar el programa que contiene el virus que en ese momento

se posiciona en la memoria de la computadora y a partir de entonces infectará todos los programas cuya extensión sea .Exe o .Com en el instante de ejecutarlos a fin de invadirlos autocopiándose en ellos. Esta operación pasará inadvertida para el usuario, pues sólo vera que la luz de la unidad de disco esta encendida, lo cual indica que se esta cargando el programa. Aunque la mayoría de estos virus ejecutables «marca» con un byte especial los programas infectados para no volver a realizar el proceso en el mismo disco, algunos de ellos se duplican tantas veces en el mismo programa y en el mismo disco, que llegan a saturar su capacidad de almacenamiento.

A más de la gran cantidad de elementos técnicos en torno a este problema, de los cuales hemos señalado algunos de los más esenciales, cabe mencionar que bajo una perspectiva económica, el tema de los virus informáticos constituye una paradoja muy singular, ya que si bien por un lado generan pérdidas económicas sustanciosas a las empresas o particulares usuarios de informática afectados por los virus, por el otro lado son varias las compañías que «capitalizan» la situación a través de las ganancias generadas con motivo de la venta de los cada vez más famosos «antivirus».

II. ORIGEN DEL VIRUS:

Se considera al virus computacional como un problema de la década de los 80's, pero la idea del virus nació desde los años 50's con la teoría de John Von Newmann, en la que hablaba de que los programas del computador podrían multiplicarse de forma alarmante; posteriormente un grupo de científicos le dieron vida a esta teoría y asi crearon «la guerra de memoria», esta fue inspirada en un programa escrito en ensamblador llamado «Creeper», el cual podía duplicarse cada vez que este corría. Para contrarestarlo, fue creado el programa «REEPER», cuya función fue la de destruir cada copia hecha por CREEPER, y autodestruirse cuando ya no existiera ningún «CREEPER».

III. CAUSAS:

Investigaciones recientes llevadas a cabo en los Estados Unidos, indican que un 70% de los virus existentes fueron realizados por personal interno y autorizado de las propias empresas. El otro 30% que es el medio mas común de contagio, son programas que entran a las instalaciones por primera vez, en copias de programas no originales.

Las tres principales causas por las que se crearon estos virus son:

1) Empleados descontentos.

2) Programadores interesados en rebasar los limites de las más reciente tecnología.

3) Empresas interesadas en la piratería de software.

IV. TIPOS DE VIRUS:

Entre las diferentes variedades de virus mas importantes conocidos hasta ahora, con especial incidencia en los equipos IBM o compatibles, tenemos, en estricto orden alfabético, los siguientes:

* AIDS también conocido como HAHAHA, MOFA y VGA2CGA
* ALABAMA
* ALAMEDA también conocido como MERRIT, PEKING, SEUL y YALE
* AMSTRAD
* ASHAR también conocido como SHOE VIRUS y VIRUS UIUC
* CASCADE también conocido como OTOÑO, LETRAS CAIDAS, 1701 y 1704
* CASCADE B también conocido como BLACKJACK y 1704-B
* BRAIN también conocido como CEREBRO PAKISTANI
* CHAOS
* DARK AVENGER
* DATACRIME también conocido como 1280 o DIA DE COLON
* DATACRIME II también conocido como 1514
* DATACRIME IIB también conocido como 1917
* DATACRIME B también conocido como 1168
* DBASE
* DEN ZUK también conocido como BUSQUEDA o VENEZOLANO
* DEVIL'S DANCE también conocido como MEXICANO
* DISK KILLER también conocido como OGRO INFORMATICO u OGRO DEL DISCO
* DO NOTHING VIRUS también conocido como VIRUS ESTUPIDO
* EDV
* FRIDAY THE 13TH COM virus también conocido como VIRUS .COM, MIAMI, MUNICH, SUDAFRICANO o VIRUS 512
* FUMANCHU también conocido como 2080 y 2086
* GHOST BOOT
* GOLDEN GATE también conocido como MAZATLAN o VIRUS 500
* HALLOPECHEN
* HOLLAND GIRL también conocido como SYLVIA
* ICELANDIC (existen 3 versiones) también conocido como CERO DE CADA DIEZ o CRUJIDOR DE DISCOS
* JERUSALEM (también 3 versiones) conocido como PLO, ISRAELI, VIERNES 13, RUSO, 1813 (COM) o 1808 (EXE)
* JOKER
* LEHIGH
* LISBON
* MIX/1

* OHIO
* OROPAX también conocido como VIRUS DE LA MUSICA
* PAYDAY
* PENTAGON
* PERFUME ALIAS 765 o 4711
* PING PONG (dos versiones) también conocido como TURIN o VERACRUZ
* SARATOGA también conocido como 642 o UNO DE CADA DOS
* SF VIRUS
* STONED tambien conocido como HAWAI, MARIGUANA, NUEVA ZELANDIA, SAN DIEGO o SMITSONIANO
* SUNDAY
* SURIV (tres versiones)
* SWAP
* SYSLOCK también conocido como 3551 o 3555
* TAIWAN
* TRACEBACK (dos versiones) tambien conocido 3066
* TYPO BOOT
* TYPO COM también conocido como TANTEO u 867
* VACSINA
* VCOMM
* VIENNA (dos versiones) también conocido como AUSTRIACO, UNESCO, DOS-62, DOS-68, 1 de 8 y 648
* VIRUS-90
* VIRUS-101
* W-13
* YANKEE DOODLE
* ZERO BUG también conocido como PALETA o 1536
* 405
* 512
* 1260
* 1559
* 1704 FORMAT
* 4096

V. EFECTOS DE LOS VIRUS:

Entre los efectos que producen los virus encontramos:

– cambia el nombre del volumen del disco,

– crea sectores malos en áreas no usadas del disco, disminuyendo paulatinamente su capacidad,

– interfieren con la operación de programas residentes en memoria RAM,

– infecta el sistema operativo,

– eventualmente cancela el BOOT y FAT (tabla de asignación de archivos) y sectores del directorio,

– provoca imágenes molestas en el monitor o envía mensajes,

– bloquea buffers de manera que no permite la entrada o salida de los discos, pareciendo una falla de software,

– daña físicamente a la computadora.

De lo anterior se desprenden dos aspectos: uno positivo ya que ahora los usuarios saben que tienen que ser mas cuidadosos y no hacer copias indiscriminadas de paquetes o discos respetando así los derechos de autor, también ahora los usuarios que han perdido toda o parte de su información debido a un virus, saben que es una práctica muy sana hacer respaldos periódicos de su información, asegurando así que la mayoría de la información estará a salvo. El aspecto negativo es el miedo al contagio de virus, evitando el intercambio de información importante que antes era fomentada, ocasionando con esto pérdida de tiempo y dinero.

VI. MEDIDAS PREVENTIVAS:

Para evitar el contagio de virus es importante:

– utilizar paquetes originales,

– tener un control de las claves de acceso,

– proteger los diskettes así como los discos duros,

– elaborar contratos laborales en las empresas contra el mal uso de los paquetes,

– tener un control de los equipos,

– realizar auditorías internas,

– programa que impide la inserción de programas «contaminados».

VII. MEDIDAS CORRECTIVAS:

El virus es una amenaza potencial a la integridad del software de cualquier computadora, debido a este problema se han creado un nuevo tipo de software «las vacunas» cuya función es detectar y eliminar el virus del disco recuperando en algunos casos la información del mismo y evitando que siga infectando otros discos.

Mas es importante tener presente que no es posible escribir un programa que detecte todos los virus concebibles, es posible construir una defensa contra cualquier virus dado y para cada defensa siempre habrá otro virus que pueda burlarla.

VIII. SEGURIDAD EN LOS CENTROS DE COMPUTO

La seguridad en centros de cómputo tiene por objeto la protección de los intereses de una organización salvaguardando el equipo, sus programas y

los datos, asegurando asi la operación confiable e ininterrumpida del sistema de cómputo.

Los especialistas en seguridad para computadoras identifican cuatro niveles o capas en la proteccion del software y el hardware.

El primer nivel, «electrónica y programación», se refiere a la protección proporcionada por los dispositivos del hardware y por las técnicas de software con que hayan sido provistos el sistema operativo, los archivos de datos y los programas de aplicación.

El segundo nivel, «protección física», corresponde por una parte a las medidas de seguridad contra incendio y fenómenos naturales y por otra, a los mecanismos que impiden el acceso al centro de cómputo y lo protegen contra atentados y robo. Asimismo, incluye a todos los procedimientos para hacer frente a contigencias.

El tercer nivel, «políticas de la organización», está constituido por los métodos y procedimientos administrativos desarrollados por la organización, en los cuales se ve involucrado el centro de cómputo.

El cuarto nivel «controles legales», consiste en la protección otorgada por las leyes internacionales, nacionales y locales y considera también los convencionalismos aceptados por la sociedad de que se trate.

La seguridad absoluta es prácticamente imposible de alcanzar en los cuatro niveles y esto se debe a la gran cantidad de elementos que componen al problema. Siendo realistas, lo que normalmente se busca al planear un sistema de seguridad es:

– minimizar la probabilidad de una falla de seguridad o una pérdida de información y,

– minimizar el daño que pudiera resultar de ellas.

El virus se manifiesta al poner en marcha el programa portador, burlando el primer nivel de seguridad. Aquí la prevención, detención y eliminación del virus corre principalmente por cuenta de programas antivirus o vacunas, aunque también es posible proteger físicamente contra escritura a algunos discos.

En el caso de destrucción de información por un virus son los procedimientos de respaldo del centro de computo, en el segundo nivel de protección, los que garantizan el restablecimiento de la información en las condiciones en que se encontraba antes de la falla.

Si bien es probable que los respaldos también están contaminados, pueden servir para rastrear, aislar y eliminar en ellos al virus.

Las medidas preventivas mas eficaces se toman generalmente en el tercer nivel de protección, donde se puede establecer una cuidadosa política para el uso de programas comerciales y del dominio público y para la conexión a redes de computadoras y centros de información electrónicos.

Todas estas acciones y otras similares brindan protección de los efectos de los virus que ingresan al sistema al intercambiar discos o recibir información por vía telefónica. Pero debe hacerse notar que los virus mas peligrosos son los de creación local, es decir, los desarrollados por los programadores del sistema. Ciertamente no son muy comunes pero representan el verdadero origen del problema y si de una vez por todas se pretendiera acabar con el, es en este punto donde deberían concentrarse los esfuerzos de prevención.

IX. ELEMENTOS JURIDICOS

Toca en turno hablar de las consideraciones legales en torno al problema de los virus informáticos. Para ello, es menester mencionar que dicha problemática a pesar de sus inevitables orígenes técnicos, tiene una connotación eminentemente económica que motiva a su vez la tutela por parte del derecho. Esto es que la pérdida o modificación de la información (o aún del sistema mismo) con motivo de la aparición de un virus informático, genera evidentemente pérdidas en lo económico (desde luego si no se cuentan con archivos de respaldo o alguna otra protección) de las cuales cabe determinar responsabilidades y hacer éstas exigibles.

Uno de los aspectos fundamentales aún no resueltos es el de regular jurídicamente la información considerada ésta como un bien intangible o inmaterial con un contenido económico intrínseco que radica en la destinación de que puede ser objeto. A falta de esto, se ha tenido que recurrir a cuestiones análogas tales como los contratos a través de cláusulas de secrecía y confidencialidad tanto en el caso de los empleados informáticos como con los proveedores de bienes y servicios informáticos.

Si bien la pérdida de información en estas condiciones puede considerarse como un riesgo informático, susceptible de eventual aseguramiento, cabe mencionar la prácticamente nula cobertura en este sentido seguramente motivada por ese carácter inmaterial de la información, lo que dificulta un cabal resarcimiento en caso de daños.

Sin lugar a dudas que una de las principales causas de la aparición de los virus informáticos, es la derivada de la piratería de los programas de cómputo que al no tener una respuesta eficaz por parte del derecho, y digo eficaz porque si bien la tendencia en estos momentos es proclive hacia los derechos de autor, siguen aún los cuestionamientos sobre la aplicabilidad de figuras tales como las patentes, yo mantengo mi parecer en el sentido de la necesaria emanación de una institución jurídica nueva totalmente particularizada, pues bien retomando la premisa inicial, es esta falta de protección que ha provocado el que «algunos» creadores de software pretendan hacerse justicia «por su propia mano» al no encontrar dispositivos reales de salvaguarda de sus intereses.

El regular o intentar regular jurídicamente este problema de los virus, nos remite de manera irremisible a los llamados «delitos informaticos», ya que finalmente, al menos en mi opinión, la responsabilidad derivada en estos casos deberá ser fundamentalmente exigida a través de una responsabilidad penal y no tanto civil, que sería mas paliativo que solución. Esta «tipificación» implica una debida identificación de los requisitos «sine qua non» como serían el sujeto activo (aquel creador o propagador de virus), sujeto pasivo (persona física o legal que resiente los daños) y el bien jurídico tutelado (los datos o información perdidas o modificadas). Por otro lado, la elaboración de un perfil delictivo en la que se especifique el carácter intencional o imprudencial de la acción, así como los casos en que se causen mayores estragos de lo pretendidos en aquello que se conoce en la doctrina penal como los delitos praeterintencionales.

X. CONSIDERACIONES FINALES

Como podemos percibir, el tema de los aspectos legales de los virus informáticos es complejo, y seguramente estas líneas breves pero espero sustanciosas no contienen los elementos de solución suficientes, sin embargo, con el ánimo de no limitarme a lo meramente enunciativo es menester sugerir la necesaria regulación de este fenómeno a través de cuerpos normativos coherentes, fundamentalmente a nivel internacional que de algún modo atenúen la cada vez mas progresiva anarquía respecto a los usos inadecuados de la computadora, en buena parte motivados por una deficiente deontología informática.

COLOQUIOS

PREGUNTA: Mi pregunta va dirigida al Sr. Castro. Si como apuntaba en su comunicación las computadoras estaban haciendo leyes en Costa Rica.

RESPUESTA DE D. JUAN DIEGO CASTRO: En este momento, –y aunque es parte del tema de la última mesa del viernes– en nuestro país hay una serie de instrumentos informáticos que nos están permitiendo hacer leyes. Desafortunadamente todavía no tenemos una computadora que haga todas las leyes. Creo que sería más barato y más eficiente que nuestra Asamblea Legislativa. Supongo que aquí eso no pasa obviamente, pero cuando digo que estamos haciendo leyes en las computadoras, desde el simple procesamiento de textos hasta una base de datos que tiene la Procuraduría con toda nuestra legislación y bases de datos específicas de Derecho Constitucional y una serie de sistemas que están permitiendo en alguna medida agilizar la producción legislativa, pero tampoco se haga ilusiones, no crea que es tan maravilloso como suena. Estamos apenas empezando. Cuando tengamos también diputados con una mentalidad un poco más del siglo XXI, creo que será mejor que tener computadoras.

PREGUNTA: La pregunta es en parte lo que acaba de mencionar el compañero, pero a la Doctora Amoroso. Aparece ella con dos temas en el proyecto que nos enviaron a nosotros ántes de este Congreso y aquí también aparece en las dos ocasiones, pero como se han cambiado los títulos, donde está el tema, probablemente la pregunta que yo le iba a hacer, va a contestarla usted cuando hable de «Legislar asistido por computadoras en Cuba». Si es que ese tema va a ser específicamente con relación a Cuba y usted que está en el Ministerio de Justicia.

RESPUESTA DE DÑA. YARINA AMOROSO: Eso lo vamos a abordar en la Mesa donde se va a tratar la aplicación de la informática al Derecho.

PREGUNTA: La Dra. Amoroso nos ha estado hablando de la protección legal del Software. Encuentro que está muy bien pero me gustaría saber la protección desde el punto de vista contrario, porque recientemente hemos sido víctimas, a través de un proceso comercial, de un programa que como

sistema de protección mucho más allá de lo legal, tenía un dispositivo que al tratar de sacar una copia pirata (no fui yo el que trató de sacarla sino la propia tienda que me vendía el programa antes de vendermelo), despertaba un virus que nos causó un destrozo en nuestro proceso particular increible. Desde el punto de vista legal sería preferible que ese sistema estuviera prohibido.

RESPUESTA DE DÑA. YARINA AMOROSO: Precisamente a esto me refería cuando decía que hay dos posiciones claras. Creo que esto de las copias «antipirata» o las copias «piratas» es un poco el reflejo de tomar la justicia por mano propia ante una ausencia de legislación. Mientras nos debatimos cual es el régimen más apropiado a la Protección del Software, en definitiva hay una realidad: Se produce software, se comercializa software, se utiliza el software y es necesario proteger tanto los bienes vinculados a esto como, incluso lo más elemental, el tiempo que se emplea para realizar una determinada aplicación o utilizar, y entonces, en tanto a esto, yo coincido plenamente con usted y por eso me refería a que hay que ir respetando todo criterio a una protección específica donde se contemple todo esto, y que también abarque la cuestión de una protección al usuario ante esta actitud indiscutible, pero que en definitiva es un reflejo de una ausencia de legislación y de una solución y por tanto, estamos en este sentido en términos un poco metafóricos ante una era de grandes resultados tecnológicos en cuanto al Derecho, un retroceso, por que se está tomando la justicia por mano propia.

(MESA N.º 5)

INTERVENCION DEL SR. JUAN DIEGO CASTRO. COORDINADOR DE MESA: Quiero agradecer a D. Emilio del Peso su intervención, así mismo agradecer y felicitar a Dña. M.ª Luz Gutiérrez, a D. Miguel Angel Gallardo y a D. Miguel Gómez por sus brillantes intervenciones.

En realidad hemos podido dar un poco acelerados por el verdugo del papelito, un paseo por una serie de facetas que surgen a consecuencia del impacto de la informática en el mundo del Derecho Penal y más que el mundo del Derecho Penal, de todas las consecuencias de carácter jurídico-penal y criminológico que tiene la aplicación de la informática en nuestra sociedad.

Coincidimos plenamente y es muy difícil resumir tan brillantes y enjundiosas exposiciones, pero los problemas que nos plantea la delincuencia informática, la criminalidad informática, van desde el problema del «iter criminis» desde el momento de ubicar las fases de tentativa y consumación en el delito informático, hasta el problema mismo de la tipicidad, el problema mismo del sujeto pasivo. Me pareció interesantísimo y coincido con ella. Ha dicho esto con todo respeto y con toda sinceridad con la posición de la profesora Gutierrez ¿Quién es la víctima de la estafa informática? Tenemos que superar el espejismo de que engañamos a la computadora. No, no engañamos a la dueña del dinero, engañamos al banco, engañamos a la compañía.

El concepto de acción en sentido jurídico-penal ¿se va a modificar o no se va a modificar con el impacto de la informática? Obviamente por el principio de legalidad, la tipicidad de los delitos informáticos tiene que ser muy bien elaborada y que ser respetada muy profundamente. El problema de la antijurisdiccidad, todo el Derecho informático, en general, no sólo en su aspecto penal, como va a incidir en causas ajenas al Derecho Penal mismo, causas supralegales de justificación en esta clase de hechos criminales. La culpabilidad misma; las características personales del delincuente informático que comentaba D. Emilio del Peso, la psicología criminológica tendrá que definirnos qué pasa con esos informáticos. ¿Será que hay falta de estímulos en la empresa? ¿Será que tienen algún otro tipo de problemas, algún otro tipo de condiciones? Toda la criminología parece que entra en crisis a raíz de las computadoras y su relación con la sociedad actual. Todo el Derecho

Penal, toda la doctrina jurídico-penal, también está en crisis y es muy importante, sin perder de vista que el Derecho Penal democrático se desarrolla y se fortalece en la medida en que también se despenalizan las conductas, es menester y aunque suene paradógico, penalizar estas nuevas conductas que atentan contra la buena convivencia social.

Quisiéramos entonces aprovechar el tiempo que nos queda, si alguno de ustedes tiene alguna pregunta que plantear a los expositores y con mucho gusto responderemos.

PREGUNTA: Es para la Doctora Gutiérrez. Yo pondría un ejemplo que se me ha venido a la cabeza, mientras estaba haciendo las instrucciones en su trabajo, yo voy al Banco con mi VISA, saco 100.000 Ptas. y en el momento de cubrir estas 100.000 Ptas. al mes que viene yo no tengo dinero, entonces ¿No cree usted que con la interpretación que usted ha hecho de la actual normativa no damos a las empresas poseedoras de tarjetas de credito, una arma abusiva para penalizar el simple impago, que sería una deuda civil?

RESPUESTA DE DÑA. M.ª LUZ GUTIERREZ: La interpretación que yo hago de la estafa, ¿es a lo que se refiere?

SIGUE LA PREGUNTA: Es dar la facultad a una empresa de tarjetas de crédito de poder discernir por sí misma, al cliente que simplemente es moroso, e interponerle rapidamente una querella por estafa.

RESPUESTA DE DÑA. M.ª LUZ GUTIERREZ: No porque para que se pueda aplicar el vigente artículo 528, según mi interpretación, (es más complejo de lo que he podido explicar aquí en unos segundos) por supuesto tiene que darse una dinámica engañosa, un comportamiento subrepticio engañoso de aquel, en el caso de la tarjeta que lo realiza. El que lo realiza de partida tiene que realizar un comportamiento subrepticio.

SIGUE LA PREGUNTA: Pero es clarísimo; hay un ánimo de lucro dirigido a gastar 100.000 Ptas.

RESPUESTA DE DÑA. M.ª LUZ GUTIERREZ: Pero es que no solamente es elemento de la estafa el elemento subjetivo ánimo de lucro. La estafa tiene una serie de elementos, un comportamiento engañoso, con actitud suficiente para producir error, al cual pueda serle objetivamente imputable el resultado de la disposición patrimonial lesiva. Con ánimo de lucro, eso solamente es un elemento. El que una persona actue con ánimo de lucro, actuamos en muchas facetas de nuestra vida. Los elementos que requiere el artículo 528 tienen que darse, así y en ese orden por el principio de legalidad penal, luego, el que solamente exista en el comportamiento de esta persona ánimo de lucro, tendremos que comprobar si existe un comportamiento engañoso, un comportamiento subrecticio suficiente dirigido a la entidad de crédito.

Suficiente atendiendo al criterio, al módulo subjetivo «Suficiente sobre esa entidad». Yo analizo si es suficiente o no comprobando las características que tendría que tener esa entidad y si es engaño sobre esa entidad, es suficiente, y ahora si ese engaño ha tenido la fuerza motora tal que ha llevado a la Disposición Patrimonial Lesiva. Si todo eso se da y además existe dolo y ánimo de lucro. El ánimo de lucro no es más que un elemento. Se tienen que dar todos los elementos. El supuesto que me ha comentado y puesto por ejemplo, solamente puede ser una estafa, pero no necesariamente. Habremos de comprobar que se dan todos los requisitos. El ánimo de lucro es sólo uno de ellos.

SIGUE LA PREGUNTA: Es decir, la idea es al revés. Dar a la empresa de las tarjetas de Créditos el poder decir: «mire, si no me paga, querella por estafa». Esta es la amenaza que el usuario en el Banco se va a encontrar con la interpretación que se ha hecho anteriormente.

RESPUESTA DE DÑA. Mª LUZ GUTIERREZ: ¿Que esa es la solución a la que se llega? A mi modo de ver, leyendo los formularios y lo que dicen mis tarjetas de crédito y los papeles que me llegan después, es muy difícil que yo engañe al banco y ellos tienen su vía para resolverlo, una vía civil. No les interesa en absoluto llegar a la vía penal. En contra de lo que se ha dicho por aquí, el Derecho Penal no es ni mucho menos el instrumento eficaz y apto para resolver este tipo de conductas. Lo que creo es que tiene una misión muy importante, que es la de crear conciencia de que eso es ilícito. La función de motivación del Derecho Penal para mi más importante que la función represiva. Ya tienen los bancos y las entidades sus propios sistemas para resarcir por la vía civil, o se traen de nuestras cuentas y compensan las pérdidas que puedan sufrir, ellos no van a sufrir, pero el Derecho Penal a mi modo de ver tiene la misión más importante de crear en el ciudadano, no solamente en los consumidores y usuarios, sino también en las propias empresas, la conciencia de que eso es un ilícito. Función de motivación penal. No es el instrumento ni más eficaz, ni el que garantiza mejor los derechos. Es el instrumento último de Control Social, el último al que hay que acudir y a mí me parece que la interpretación a la que hecho referencia de la estafa, que aquí no puedo simplificar porque realmente la he tenido que simplificar demasiado, no lleva a castigar como estafa los comportamientos a los que usted ha hecho referencia.

PREGUNTA: Esta pregunta es para la Doctora M.ª Luz Gutiérrez. En la estafa, digamos clásica, si se verifica mediante documento falsificado, tenemos dos delitos, el de estafa y el de falsedad. En caso de tarjeta de crédito que no sea sustraída, sino manejada en su banda magnética, el proyecto de Código Penal, ¿Tendría también tipicación como estafa y falsedad o solamente estaría englobado en un sólo delito?.

RESPUESTA DE DÑA. M.ª LUZ GUTIERREZ: En las falsedades documentales ahora hay un problema doctrinal sobre cuál es el tratamiento cuando se realizan las estafas a través de las falsedades en documento público o en documento privado. Quiero decir que si es un documento público, como será este caso, sería un concurso de delitos con una falsedad en documento público más el delito de estafa. En relación con los delitos de falsedades, yo he apuntado también brevemente, que no se hace ninguna referencia a las falsificaciones cometidas por medios informáticos, luego esa materia, que está absolutamente vinculada en supuestos como el que acaba de comentar usted, que está absolutamente vinculado con los fraudes informáticos, eso queda en el aire, o sea, se deja al momento de la reforma penal y ahí deja una laguna las falsificaciones por medios informáticos, como un caso que traía yo aquí que luego no lo he comentado, del 89, unos jóvenes que falsifican la banda magnética de unas libretas de ahorro. ¿Qué pasa?, si son las libretas de ahorros se falsifican la banda magnéticas para cometer una estafa ¿esto ya no está incluido dentro de las tarjetas electromagnéticas porque no son tarjetas?. Todo eso deja aquí una laguna tremenda el legislador. Yo tengo aún la secreta esperanza de que esto entre en el debate parlamentario y sea objeto de una reforma y se superen estas lagunas, porque incluir un delito de estafa informática y dejar el vacío al lado de las falsedades por medios informáticos, me parece imperdonable.

PREGUNTA: Yo quería preguntar a la profesora de Derecho Penal de Salamanca y también al profesor de La Laguna. Yo soy también penalista y me ha sugerido una pregunta.

En cuanto al bien jurídico protegido, el tema que yo creo que es problemático en la informática, es la cuestión que como bien han apuntado realmente, ¿En qué título del Código Penal podríamos introducir los delitos contra la Informática?. Por que si observamos, existe bien juridico protegido por un lado el Derecho a la intimidad, pero Vd., por ejemplo, su tesis va sobre el fraude informático. Ahí no tiene nada que ver, por ejemplo, con el bien jurídico del Derecho a la intimidad. Aquí estamos hablando de delitos socio-económicos. Si por otro lado tenemos en cuenta la conducta que atenta contra los elementos informáticos, entonces es otro bien jurídico diferente o al menos otro tipo dentro de los delitos socio-económicos, por eso digo yo que es una cuestión compleja que no sería susceptible de ser introducida sólo en un título del Código Penal.

En cuanto a lo que decía el profesor de La Laguna de la cuestión de como distinguimos la naturaleza jurídica del tipo penal, qué es, ¿un delito de resultados o un delito de simple actividad?. ¿Cómo distinguimos entonces los actos preparatorios no punibles de la tentativa o consumación que ya si son punibles?. Realmente es que sería necesario un debate de fondo muy fuerte para ser capaces de sistematizar a ver donde metemos cada conducta

y también sin atentar contra el principio de intervención mínima, porque habrá situaciones que no se requiera que intervenga el Derecho Penal, ello en consonancia con el principio de última ratio y de intervención mínima.

Respecto a lo que decía el coordinador, qué creemos que es el Sr. Gallardo, yo creo que más bien es un filósofo que mantiene una actitud escéptica ante este tema porque realmente la cosa está cruda.

RESPUESTA DE D. MIGUEL GOMEZ: Hay omisiones que he cometido forzosamente, otras inconscientemente.

Hay que tener presente muchas cuestiones. El principio de intervención mínima, quería aludir a él, también quería concluir viendo ante la situación real delictiva, todavía no típica, pero sí de situaciones conflictivas, ¿Qué soluciones ofrece el Derecho?. La ley de propiedad intelectual, la industrial y la penal propiamente, y dentro de la penal distinguir que vías hay que adoptar ahora, si crear nuevos tipos totalmente nuevos, o mejorar los ya existentes, los daños serán retocados en el anteproyecto para facilitar el que los delitos informáticos puedan ser incluídos.

Respecto a la segunda pregunta, es una cuestión de política criminal, es decir, si se prefiere configurar un tipo, en el caso que se legalice la situación como de simple peligro, o se prefiere tipificarlo como de resultado y coherente con ello, tendremos que los tres momentos, el que se produzca el evento condicionante de que esa rutina opere, es decir, el empleado de una empresa que teme ser despedido; en el momento del despido y en el momento en que opera la rutina sobre el programa, entonces son dos momentos que marcan dos lapsus de tiempo, un primer momento de una actividad preparatoria no punible, en el momento en que se introduce la rutina si consideramos que la comisión se producirá solamente cuando se produzca el resultado: la lesión. En cambio si consideramos que es de simple peligro, ya al introducir la rutina oculta lo está creando. La respuesta es que depende de la configuración como de simple resultado, de simple actividad o de resultado, los momentos (de preparación, de tentativa y el de consumación) van a variar, pero es simplemente eso, según el legislador opte política o criminalmente más conveniente tipificarlo cuando se tipifique.

Es una cuestión de política criminal. El efecto ha de ser coherente, es el de que se desplazan los momentos y las calificaciones de esos lapsos, es decir, la tentativa empezará en un momento determinado y no ántes. En relación al resultado será, si es delito de resultado, posterior a si es de simple actividad en que el peligro comienza antes, y la consumación también se produce antes.

RESPUESTA DE DÑA. M.ª LUZ GUTIERREZ: Yo detecto en su planteamiento un problema de fondo y es que habla de delito informático. En ningún momento se puede hablar de delito informático, sino de una manifestación de la criminalidad, o sea, es un fenómeno criminal complejo, heterogé-

neo que tiene muchas manifestaciones, sin una categoría unívoca dentro del Derecho positivo, pero que tampoco debe tener pretensiones de tenerla.

Yo al hablar de las defraudaciones, del fraude informático, no lo hago con pretensiones de que en un futuro haya un tipo de fraude informático, porque a mi modo de ver, el fraude informático y mucho más la delincuencia informática en su conjunto, puede contemplarse como una categoría única, unívoca y que haya de ser tratada como un único bien jurídico, un único comportamiento típico, una única ubicación sistemática, ni mucho menos. Es un fenómeno criminal, es una manifestación de la criminalidad moderna que ha de ser abordada desde distintas perspectivas que ¿cómo ha de ser tratada?, tenemos distintos modelos: El modelo alemán que ha dejado el código tal y como estaba y que ha metido dentro de los delitos de apoderamiento material tal materia, el concepto de llave falsa dentro de la estafa, la estafa informática, dentro de las falsedades, la falsedad por medios informáticos, dentro de los delitos contra intimidad, etc.

Y luego existen otros modelos, como el modelo francés que lo que hace es recoger en un capítulos todo los supuestos de atentados contra medios informáticos que entrarían en concurso con cada una de las figuras penales, siempre que se intercepte un sistema informático, se manipulen sistemas informatizados, se manipulen datos en los programas, etc., o se abuse con tales y tales comportamientos, y en un título independiente se regulan todas las conductas. Si se realiza una estafa con cualquiera de esos medios entra en concurso de delitos; si se realiza un hurto o delito de daños con esos medios, entra en concurso, tenemos dos posibilidades. A lo mejor nosotros nos inventamos otra.

Ya es un error hablar de delito informático en singular. Delito es una categoría demasiado técnica para que se utilice en singular, cuando no existe en el Código Penal nada que sea delito informático. Si no lo consideramos categoría criminológica, ni si quiera debemos hablar de delito, sino de delitos, o de hechos ilícitos porque todavía no están tipificados.

INTERVENCION DE D. JULIO TELLEZ: Con motivo de una de las preguntas que flotaban en el ambiente, al menos la posición que sostengo es que el Bien jurídico tutelado pudiera estribar en la información. En este sentido, un bien tangible está debidamente contemplado, como puede ser el caso del robo, como el apoderamiento físico de una cosa mueble. Sin embargo si la información la consideramos como un bien intanglible, inmaterial, con un contenido económico intrínseco que radica, en cuanto a la destinación de que puede ser objeto, ahí es donde podemos en última instancia, identificar la posibilidad de ese bien jurídico tutelado, de tal manera que, insisto, en los

Códigos Penales tendrían que darse las reformas suficientes para incorporar a esos bienes intangibles o inmateriales, que, desde luego, no sería nada nuevo porque figuras jurídicas como las patentes, los derechos de autor, surgieron con motivo de la revolución industrial, y de algún modo dan la pauta a pensar que esta revolución informática en la que estamos inmersos, también debe propiciar, a su vez, un nuevo orden jurídico.

SESION IV

MESA N.º 6.–REGULACION JURIDICA DE LA INFORMATICA Y LAS TELECOMUNICACIONES

Utilización de la informática en la detección de comportamientos irregulares en los mercados de valores

JOSE M.ª DE PAZ ARIAS

Licenciado en Derecho. Doctorando en el Area de Derecho Mercantil de la Facultad de Derecho de Zaragoza (ESPAÑA)

La utilización de medios informáticos en la detección de transacciones de valores que revelen la existencia de operaciones «irregulares», como el uso de información privilegiada, la manipulación de cotizaciones o la adquisición, omitiendo la obligación de comunicación, de paquetes significativos de acciones, proporcionaría indicios razonables acerca de la realización de actuaciones que pretenden mantenerse ajenas a la obligación de transparencia que impera hoy en los Mercados de Valores, tales como la citada comunicación de los porcentajes adquiridos en el capital de sociedades cotizadas (Real Decreto 377/1991).

Estos procedimientos son especialmente adecuados en el caso de mercados absolutamente informatizados, como es nuestro Mercado Continuo, ya que todo movimiento, toda operación realizada en el seno de estos mercados queda automáticamente registrada en el propio sistema, el cual proporciona información acerca del volumen de las transacciones, el tiempo de realización de las mismas, la prioridad de las órdenes y los operadores implicados.

De hecho, mecanismos de esta naturaleza vienen siendo empleados en la Bolsa de New York, en la que existe un conjunto de ordenadores capaz de detectar cuándo un valor está negociándose en volúmenes anormalmente altos o está subiendo de forma inesperada. Cuando un valor excede su volu-

men de transacciones y su precio rompe las barreras de ciertos porcentajes de subida, ello queda detectado en la impresora. Evidentemente, el sistema informático proporciona tan solo un indicio, un punto de partida a partir del cual el análisis humano interpreta los datos y considera la posibilidad de iniciar una investigación que puede desembocar en la localización y consiguiente represión de una conducta prohibida. Este sistema ha obtenido éxitos significativos en su contribución a la lucha contra el abuso de información privilegiada, como fue el caso Levine y Boesky, en que la detección de un incremento anormal de precios y volúmenes de cotización de la empresa «American Natural Resources» en marzo de 1985 condujo a la iniciación de una investigación por parte de la Comisión de Valores y Bolsa, investigación que terminó con las actividades delictivas de estos dos especuladores.

El estudio en España de estas técnicas informáticas de control se ha de centrar, fundamentalmente, en el sistema de Mercado Continuo, dada su completa informatización y, sobre todo, por la preponderancia que ha adquirido en el mercado de valores desde su implantación (en 1991, de hecho, el 86% del total negociado se hizo a través del Mercado Continuo).

Tomando como presupuesto la utilidad del empleo de medios informáticos, la dificultad se plantea al intentar establecer algún criterio discriminador respecto a la información recogida por los ordenadores que registran las operaciones del Mercado Continuo.

En primer lugar conviene no perder de vista que cada una de las operaciones que se pretenden controlar obedecen a motivaciones y presentan modos de aparición en el mercado diferentes.

Si de empleo de información privilegiada se trata, el dato esencial reside en la utilización, en un momento determinado, de una información que, dirigida al mercado, va a tener una influencia sensible en el precio de determinados títulos, de modo que esa diferencia temporal permita al conocedor de la misma comprar o vender en la Bolsa disponiendo de un factor de decisión del que carecen los restantes operadores.

En el caso de tomas de participación significativas, en el sentido tanto del Real Decreto de 15 de marzo de 1991 como en el de 26 de julio del mismo año, la intención del adquirente puede ser tanto la puramente especulativa, como el inicio de una operación de control. Pero en ambos casos es posible detectar un grado de estabilidad en la posesión de los títulos del que carece el «insider» o «iniciado», sin que con ello queramos decir que una operación de toma de participación significativa no se pueda combinar con elementos típicos de la figura del «insider trading», o que la operación concluya con una toma de control que se pretende transitoria.

Por último, en los supuestos de manipulación de las cotizaciones de lo que se trata es de, en definición de Núñez-Lagos, alterar el curso ordinario de la oferta y la demanda mediante artificios que la estimulen o depriman.

Detrás de estas manipulaciones se pueden encontrar motivos que van desde la pura ganancia especulativa hasta el deseo de la propia sociedad cotizada de impedir una baja generalizada de su cotización a través de una intervención en el mercado adquiriendo sus propios títulos y, consiguientemente, ampliando su autocartera.

En cualquier caso, estas tres operaciones tienen reflejo en dos datos fundamentales: el precio de cotización del valor y el volumen de contratación del mismo. La incidencia en ambos es diferente según el supuesto ante el que nos encontremos.

Si tomamos el ejemplo del uso de información privilegiada, el dato clave reside en el hecho de que la información en que se basa la actuación del iniciado debe llegar tarde o temprano al mercado. Por tanto, la detección del momento en que la noticia (vgr. la formulación de una oferta pública de adquisición de valores) entra en la Bolsa y comienza a difundirse resulta de importancia capital, pues nos permite introducir un punto de inflexión en la evolución de las cotizaciones del valor y analizar el comportamiento del valor en los días o semanas inmediatamente anteriores.

En el caso de manipulación de valores la dificultad de detección de la misma corre pareja a la diversidad de medios a través de los que se produce tal manipulación. Así, es posible proceder a esta manipulación mediante compras y ventas de un valor que no respondan a la situación real del mercado, mediante la difusión de falsedades o mediante ventas falsas previamente convenidas.

En los supuestos en los que se pretende la adquisición de un número de títulos suficiente como para conceder el control de una sociedad cotizada, los factores a considerar residen, por una parte, en el volumen de títulos que se adquiera a lo largo de un período de tiempo, y, por otra, en el o los adquirentes de dichos títulos. La consideración conjunta de ambos factores nos permite obtener una caracterización completa del modo de presentación de esta conducta.

Por supuesto, en este caso estamos excluyendo las cesiones privadas de control, ya que en este caso la venta de los títulos se produce fuera de Bolsa y ello, con independencia de que se violen o no las obligaciones prescritas por la legislación sobre Mercado de Valores tanto en la ley como en su desarrollo reglamentario, implica que los medios informáticos carecen de eficacia al no tener lugar la transacción a través de los mismos.

En orden a la formulación de un criterio discriminador de la información recopilada las posibilidades son varias. Hemos de tener en cuenta que el objetivo de este estudio se centra en el uso de la informática como instrumento que permita detectar indicios razonables de que en el mercado se están o se han producido conductas que afectan a su funcionamiento y a la confianza que los inversores tienen depositada en él. Pretender formular criterios

que nos proporcionen una certeza absoluta acerca de la realización de estas conductas resulta imposible, entre otras razones por la inexistencia de unos parámetros que dibujen el comportamiento «normal» de los Mercados de Valores.

Uno de los criterios que podrían introducirse en orden a la detección de una conducta irregular sería el desplazamiento de elementos como la cotización o el volumen de negocio del valor respecto de su posición habitual. El problema de este método reside en la imposibilidad de establecer de modo genérico cuál va a ser el comportamiento «normal» de un valor en el mercado. Se ha comprobado que ni el análisis técnico, ni el fundamental nos proporcionan una seguridad lo suficientemente elevada en cuanto a la predicción en el alza o baja de la cotización de un valor (en ello se basa la aparición del tercer sistema, el Random Walk), con lo que la fijación del modelo de comportamiento respecto del cual la desviación en el volumen de contratación o en la cotización nos proporciona un indicio resulta complicado.

Pese a ello, la aplicación de un criterio cuantitativo resulta lo suficientemente provechoso como para afrontar las dificultades apuntadas. Por ello cabe sugerir que se establezcan unas tablas de variaciones no demasiado complejas que permitan su aplicación con un mínimo de eficacia y rapidez.

Otra posibilidad reside en la conexión informática de todos los ficheros de clientes y las órdenes de compra y venta de los mismos que forzosamente han de llevar los operadores oficiales en el mercado. En este sentido, el Texto definitivo del Proyecto de Real Decreto sobre normas de actuación en los Mercados de Valores y Registros Obligatorios establece en su capítulo III, dedicado a los registros obligatorios y relaciones con la clientela, la obligación de que las Sociedades y Agencias de Valores dispongan de un registro de operaciones, llevado por medios informáticos, en que se recoja toda la información sobre las órdenes recibidas, incluyendo el conocimiento exacto del orden de recepción de las mismas y de su fecha y hora.

Junto a este archivo de órdenes, se establece que «toda persona, entidad o establecimiento habilitado para actuar como receptor material de órdenes sobre alguna de las actividades relativas a la actividad de intermediación y depósito de cualesquiera valores deberá mantener un archivo de justificantes de las órdenes recibidas», archivo que estará formado por el ejemplar original de la orden firmada por el cliente o persona autorizada, la cinta de la grabación cuando sea realizada de modo telefónico o el registro correspondiente en el caso de transmisión electrónica. Así mismo, las entidades dispuestas a aceptar las órdenes por vía telefónica no escrita deberán establecer los medios necesarios para la identificación de sus ordenantes.

En tercer lugar, se habilita a la Comisión Nacional del Mercado de Valores y al Banco de España para acceder al registro de operaciones y al archivo de justificantes de órdenes, con el cual se cierra el mecanismo de control y

alcanzamos, de facto, una nominatividad absoluta en la transmisión de valores, pudiendo identificarse de esta forma los emisores de órdenes de compra o venta.

Sin embargo, este segundo sistema no puede ser, hoy por hoy, sino un elemento de actuación subsidiario una vez que se sospecha la existencia de alguna irregularidad. Es preciso la existencia de un indicio para que la Comisión Nacional del Mercado de Valores proceda a la investigación del registro de órdenes y del archivo de justificantes. Por tanto, reconociendo que una vez iniciada la investigación la existencia de estos medios va a facilitar enormemente la labor, hemos de volver al primer punto, es decir, a la posibilidad de determinar un parámetro conforme al cual establecer que se está realizando alguna conducta irregular en el mercado.

Otra propuesta podría consistir en la adopción de la teoría de los «estudios de acontecimientos» o «event studies» (Arruñada, 1990).

Esta teoría aísla el efecto que sobre el valor de las acciones tiene un acontecimiento determinado, para lo cual elimina el efecto que tengan los fenómenos comunes a todas las demás empresas del mercado y los hechos ajenos al acontecimiento y que afectan específicamente a cada empresa. Con esta técnica es posible detectar los rendimientos anormales medios para los períodos de tiempo anteriores y posteriores al acontecimiento, así como el rendimiento anormal acumulado para cada uno de esos períodos.

Este método proporciona una serie de evidencias empíricas de gran utilidad, ya que si es posible aislar la incidencia en el valor de unas acciones de los diferentes factores que intervienen, por exclusión se puede alcanzar la conclusión de que ha entrado en juego un factor que no puede ser determinado en función de la información disponible en el mercado, lo cual implica un indicio que puede conducir a pensar en el uso posible de información privilegiada.

Sin embargo, este método presenta dos inconvenientes. En primer lugar es el resultado de un complicado análisis que, por ello mismo, no es susceptible de aplicar de modo generalizado a todas las operaciones que se produzcan en el Mercado, aunque no cabe duda de su utilidad en el análisis de los datos una vez confirmada la existencia de una conducta irregular y de una variación en los precios o en la cotización que no se corresponde a la información existente en ese momento en el mercado. En segundo lugar, esta teoría tiene como condición de aplicación la existencia de un Mercado eficiente, requisito que resulta arriesgado afirmar que se cumple en el Mercado español.

Con el término Mercado eficiente estamos haciendo referencia a la existencia de un mercado que se ajuste a la «hipótesis del mercado de capitales eficiente» (the efficient capital market hypothesis), y que consiste en la idea de que «los precios de los valores mobiliarios incorporan toda la información

relevante y disponible, tanto sobre el valor de que se trate como sobre el mercado en general» (García de Enterría, 1989).

Como se puede observar, las dificultades que se plantean en la aplicación de los criterios formulados no dejan de ser notables. Tal vez el error consista en la búsqueda de un único criterio aplicable a toda la información que se recoja. Hemos de tener en cuenta que cada uno de los tres criterios formulados opera sobre datos diferentes. El criterio cuantitativo sobre el volumen de contratación y negocio del valor en cuestión. La interconexión de los ficheros de las Sociedades y Agencias de Valores sobre los datos de órdenes y clientes recogidos en los mismos. La teoría de los «event studies» sobre un amplio número de informaciones que circulan en el mercado.

De este modo no resulta difícil concluir que la solución más acertada consiste en una combinación de los tres métodos. Esto es, comenzando por la introducción de un umbral de negociación y de precio de cotización cuya superación implique la puesta en marcha de un mecanismo de inspección por parte de la Comisión Nacional del Mercado de Valores, pasando después a la aplicación, si es posible en nuestro país, de la teoría de los «event studies» para aislar el factor que ha dado lugar a ese alza del precio, y, si se concluye que hay un elevado número de posibilidades de que se trate de alguna conducta irregular, la consulta de la base de datos que contenga la información acerca del intermediario o intermediarios que introdujeron las órdenes en el sistema para, a través de ellos, llegar a los ordenantes.

Sin embargo, frente a esta descripción de lo que podría ser una aplicación ideal de mecanismos informáticos en la detección de determinadas conductas, se alza una realidad compleja, en permanente mutación, como es la de los Mercados de Valores. No es éste el lugar apropiado para describir de manera pormenorizada los medios de los que disponen los intervinientes en el Mercado para evitar la aplicación de la regulación pertinente, pero se proporcionaría una imagen errada de lo que puede suponer la introducción de éstos u otros mecanismos similares si no se indicase que los medios para neutralizar su eficacia también existen. En cualquier caso, la introducción de estos métodos ha demostrado su eficacia en la práctica, por lo que, pese a los reproches que se puedan formular, no cabe duda de que proporcionan un grado de confianza y de seguridad al Mercado nada despreciables, amén de constituirse en un instrumento auxiliar para el trabajo de las autoridades supervisoras.

Pasando al terreno de las conclusiones, creo que la primera de ellas se centra en el reconocimiento de que la aplicación de mecanismos informáticos en los Mercados de Valores sólo puede tener un valor indiciario, sin que sea posible que nos proporcionen siempre y con una completa seguridad la pista que nos permita llegar a la represión de todas las conductas prohibidas.

En segundo lugar, una vez aceptadas las ventajas que la implantación de estos mecanismos ofrecen, es preciso reconocer que el método de detec-

ción basado en criterios cuantitativos constituye el de más simple implantación, el más válido y flexible como piedra angular del sistema, aunque su eficacia pueda quedar en entredicho si se pretende que vaya más allá de su capacidad, tal y como se ha descrito.

En este sentido, la elección del criterio de discriminación de la información, esto es, de los umbrales de cotización o de volumen de cotización a partir del que los ordenadores registren la posible existencia de un comportamiento irregular, es algo que dependerá de un análisis acerca de cuál es el comportamiento habitual del mercado y a partir de qué límites se puede considerar que se ha producido una alteración anormal, cuestión de gran complejidad si tenemos en cuenta la dificultad que ello supone en un Mercado en que la aleatoriedad es la norma, si es que atendemos a las últimas teorías al respecto.

Junto al cuantitativo, la utilización de los demás métodos apuntados, bastante más complejos, pueden constituirse en auxiliares que entren en funcionamiento una vez que se sospeche la existencia de un caso de uso de información privilegiada o de manipulación de cotizaciones.

Por lo demás, y en relación con la posibilidad de una interconexión entre los ficheros de clientes y órdenes de las Sociedades y Agencias de Valores, la conclusión extraída se condiciona a que el Texto definitivo del Proyecto de Real Decreto sobre normas de actuación en los Mercados de Valores y Registros Obligatorios no sufra modificaciones sustanciales, al menos en los aspectos en los que los hemos considerado, en su tramitación parlamentaria.

BIBLIOGRAFIA

ARRUÑADA, B. «Control y regulación de la sociedad anónima», Madrid, *Alianza Economía y Finanzas* 1990.

GARCÍA DE ENTERRÍA, J. «Sobre la eficiencia del Mercado de Capitales. Una aproximación al Securities Law de los Estados Unidos», *Revista de Derecho Mercantil*, 1989.

PRAT RODRIGO, M. «El uso ilegal de información privilegiada en las ofertas públicas de adquisición de acciones (EE.UU. 1933-1988)», Bilbao, Deusto, 1990.

El Derecho Comunitario de las Telecomunicaciones

JOSÉ M.ª GIMENO FELIÚ

Profesor Ayte. de Derecho Administrativo en la Facultad de Ciencias Económicas y Empresariales de la Univ. de Zaragoza

VITELIO M.ª TENA PIAZUELO

Profesor asociado de Derecho Administrativo en la Facultad de Derecho de Zaragoza

(ESPAÑA)

En las líneas que siguen se pretende hacer una sucinta referencia al régimen jurídico de las telecomunicaciones y a la creciente intervención de la Comunidad Económica Europea en esta materia, considerada como elemento esencial de cara a la consecución del objetivo de un Mercado Unico a partir del 1 de enero de 1993.[1] Intervención comunitaria que, presidida por la idea de la liberalización para aumentar la competencia, va a significar un desmantelamiento de los tradicionales monopolios existentes en el sector. Al respecto merece la pena recordar que las telecomunicaciones se han desarrollado en Europa como servicio público gestionado por organismos públicos, resultado de una política socio-económica en la que el control por parte del Estado de determinadas actividades o sectores económicos –p. ej. banca, energía o telecomunicaciones– resulta trascendental de cara a la consecución del interés general.[2]

---

[1] Como señala (JACQUES DELORS, 1990) será un mercado único para todas las actividades económicas.

[2] (G. ARIÑO ORTÍZ, 1981). Se asiste, de cualquier forma, a un creciente proceso privati-

Pues bien, la política comunitaria en esta materia se orienta hacia dos objetivos: abrir los mercados nacionales a la competencia y, como complemento, elaborar normas comunitarias de armonización y reconocimiento mutuo de especificaciones técnicas nacionales, que permitan eliminar la diversidad de normas y procedimientos nacionales. Todas estas medidas comunitarias tienen su origen en el «Libro Verde» de las Telecomunicaciones, publicado el 30 de junio de 1987 por la Comisión Europea, en el que, con carácter consultivo, se recogen los principios fundamentales para la liberalización y armonización de las telecomunicaciones. [3]

Con posterioridad a la entrada en vigor de la LOT se han aprobado una serie de disposiciones comunitarias que habrán de ser incorporadas a nuestro Ordenamiento jurídico. Básicamente, las finalidades que persigue la Comunidad se resumen en evitar las barreras tecnológicas entre las redes europeas de telecomunicación, así como procurar la libre competencia en todos los servicios de valor añadido. Se pretende con ello una liberalización del mercado de las telecomunicaciones para con dicha apertura beneficiar a los usuarios de estos productos. Con este fin, la Comisión ha publicado en 1990 un segundo Libro Verde que aborda de manera más específica las telecomunicaciones vía satélite.[4]

En el proceso de liberalización de los servicios de telecomunicación, con el objetivo de introducir una mayor competitividad, la Comisión, al amparo del art. 90 TCEE, ha aprobado estas dos Directivas:

a) Directiva 90/387/CEE, de 28 de junio de 1990, relativa al establecimiento del mercado interior de los servicios de telecomunicaciones mediante la realización de la oferta de una red abierta de telecomunicaciones, que tiene por objetivo armonizar las condiciones para el establecimiento de una red abierta de telecomunicaciones, objetivo fundamental para la realización de un mercado único de servicios de valor añadido.[5]

Se trata de una Directiva-Marco[6] que regula los principios básicos de

---

zador y desregularizador general y, en particular, de este concreto campo económico de las telecomunicaciones. Al respecto, por todos, vid. (R. MARTÍN MATEO, 1988).

[3] Son diez los principios enunciados por la Comisión, tendentes a lograr la liberalización del sector –tradicionalmente cerrado– a la vez que aumentar las posibilidades de supervisión y control por parte de la Comisión, a fin de garantizar el cumplimiento de las normas de la competencia. Como se dice en el Libro Verde, la Comunidad desea y debe tener una infraestructura de redes eficaz y unas administraciones de telecomunicaciones fuertes en un ambiente de concurrencia. En relación a contenido y objetivos del Libro Verde, vid. (R. SCHULTE-BRAUCKS, 1990).

[4] COM(90), 490 final. El objetivo de dicho documento es ampliar la aplicación de los principios generales de la política comunitaria de las telecomunicaciones a las comunicaciones por satélite, para lo que se propone, fundamentalmente lo siguiente: la liberalización completa del sector terrestre, el acceso libre a la capacidad espacial, la libertad comercial total para los proveedores del sector espacial y la armonización necesaria para facilitar el suministro de servicios a escala europea. Sobre esta última cuestión puede consultarse a (H.P. GEBHARDT, 1991).

[5] DOCE n.º 12, de 24 de julio.

[6] Fundada en el art. 100 A del Tratado de la CEE, que establece, tras la modificación operada en el Acta Unica, el llamado procedimiento de «cooperación con el Parlamento Euro-

la Red Abierta de Telecomunicaciones, entre los que anotamos que las condiciones de acceso a la red estarán armonizadas para toda la CEE, y se basarán en criterios objetivos, públicos y no discriminatorios; y que el derecho de acceso será igual para los nacionales que para los ciudadanos de otros Estados miembros.[7] Lograr el reconocimiento recíproco entre los Estados de que sus procedimientos de adjudicación de licencias permita automáticamente operar en toda la Comunidad (el denominado principio «one-stop shop»), se plantea como un objetivo importante.

b) Directiva 90/388/CEE, de la Comisión, de 28 de junio de 1990, relativa a la competencia en los mercados de servicios de telecomunicaciones.[8] Esta Directiva, con fundamento en el art. 90.3 del Tratado, pretende la liberalización del mercado de servicios de telecomunicación, y se justifica por las numerosas restricciones que los Estados miembros vienen imponiendo a la utilización de la infraestructura de telecomunicaciones por parte de otros proveedores de servicios de telecomunicaciones. La disposición fundamental de la Directiva es la obligación que se impone a los Estados de eliminar los derechos especiales o exclusivos que se hayan establecido con respecto a la oferta de servicios de telecomunicaciones distintos de los de telefonía vocal y télex.[9] Desde la entrada en vigor de esta Directiva (en principio, el 1 de enero de 1993) las empresas privadas podrán ofrecer los servicios de valor añadido en absoluta concurrencia en toda la Comunidad Europea. Igualmente podrán ofrecer servicios de conmutación de datos por paquetes o por servicios mediante la simple reventa de la capacidad de las líneas alquiladas.[10] Estas dos Directivas constituyen las dos principales decisiones para la creación de un verdadero mercado interior y armonizado abierto a la competencia en el sector de las telecomunicaciones.

Debemos, no obstante, hacer mención a otras dos Directivas:

– La Directiva 89/552/CEE, del Consejo, de 3 de octubre de 1989, relativa a la coordinación de determinadas disposiciones legales reglamentarias y administrativas de los Estados miembros sobre el ejercicio de actividades

---

peo», conforme al cual se habilita al Consejo para adoptar, mediante mayoría cualificada (ya no por unanimidad), las medidas necesarias para el establecimiento y funcionamiento del mercado interior. Sobre esta cuestión puede consultarse a (H.J. GLAESNER, 1989).

[7] Al respecto debe tenerse en cuenta la Comunicación de la comisión al Consejo y al Parlamento sobre la necesidad de potenciar las redes transeuropeas en los sectores de transporte, energía y telecomunicaciones. COM (90) 585 final, de 23 de enero de 1991: «Hacia unas redes transeuropeas. Programa de actuación comunitaria». Y es que, como bien señala (J. CHEVALIER, 1991) la comunitarización de las redes tiende a hacer caduca la idea del proteccionismo y a derribar las estructuras monopolísticas heredadas del pasado.

[8] DOCE Serie L núm. 192, de 14 de julio de 1990.

[9] Sobre el contenido y alcance de las dos Directivas citadas, (CORTINA NAVARRO Y DE CARLOS BELTRÁN, 1992).

[10] La Comisión publicó con posterioridad las líneas directrices relativas a la aplicación de las normas sobre la competencia de la Comunidad en el sector de las telecomunicaciones y que tienen por objeto aclarar la aplicación de las normas a los operadores de este sector. DOCE C 233, de 6 de septiembre de 1991.

de radiodifusión televisiva, y que tiene por objetivo tanto garantizar las condiciones que permitan a todos los residentes de la CEE tener acceso a todos los programas de la CEE que hayan surgido gracias a las tecnologías de retransmisión por cable y vía satélite, como suprimir los obstaculos a este libre acceso.

– Directiva del Consejo 91/263/CEE, de 19 de abril, relativa a la aproximación de las legislaciones de los Estados miembros sobre equipos terminales de telecomunicación, incluido el reconocimiento mutuo de su conformidad, y cuyo objetivo es la realización del mercado único de los equipos terminales de telecomunicación mediante la aplicación de procedimientos armonizados de certificación, comprobación, marcado, garantía de calidad y vigilancia de los productos, con el fin de garantizar el cumplimiento de los requisitos esenciales ya especificados en la Directiva 86/361/CEE del Consejo. Así, se establecen los requisitos esenciales que deben cumplir los equipor terminales, no pudiendo los Estados miembros impedir la comercialización, libre circulación y uso en su territorio de los equipos que cumplan con dichos requisitos.

Finalmente, se debe recordar la notable intervención de la CEE en los procedimientos nacionales de contratación pública en materia de telecomunicaciones, habiendo sido aprobada al respecto la Directiva 90/351/CEE, del Consejo, de 17 de septiembre de 1990, cuyo umbral de aplicación –es decir, el montante económico por debajo del cual no es exigible la publicidad en el DOCE– son seiscientos mil Ecus en el caso de suministro y cinco millones en los contratos de obra.[11] En esta Directiva, de ámbito realmente extenso, se establecen determinadas condiciones de contratación a fin de garantizar la transparencia e igualdad en la adjudicación.[12] Su objetivo final es lograr una mayor concurrencia real en este sector, tradicionalmente cerrado a las empresas extranjeras –incluso comunitarias– para favorecer a las nacionales.[13] Sin profundizar más en el contenido de las normas citadas, tarea imposible sin desbordar el propósito introductorio de estas páginas, cabe concluir valorando en conjunto la importancia de estas Directivas, por cuanto demuestran el inevitable avance del proceso de comunitarización de las distintas políticas

[11] DOCE Serie L núm. 297, de 29 de noviembre de 1990.

[12] Sobre esta cuestión, (F. DIEZ MORENO, 1990); (SAMANIEGO BORDIU, 1991); y (SANTIAS VIADA, SANTAMARÍA DE PAREDES Y LÓPEZ BLANCO, 1991).

[13] Baste recordar en este punto la Comunicación de la Comisión sobre «El Régimen comunitario de la contratación pública en los sectores excluidos: agua, energía, transporte y telecomunicaciones», COM (88) 376 final, donde se señala que entre el setenta y el noventa por ciento de los contratos de telecomunicación se atribuyen a empresas nacionales. Como señala (A. MATTERA, 1991) la contratación pública ha sido un instrumento en manos de los poderes públicos para realizar una política de intervención en la vida económica, social y política del país. Recuérdese, a este respecto, como el art. 84 bis de la Ley de Contratos del Estado excluye la obligatoriedad de la publicación del anuncio de licitación en el DOCE, entre otros, en los contratos de suministro convocados por los organismos públicos que gestionen servicios de telecomunicaciones.

nacionales.[14] Objetivo ciertamente importante que ha de suponer un mayor ámbito de juego de la libre competencia a fin de obtener un mayor nivel de eficiencia económica y de competitividad frente a los países no comunitarios, con la consiguiente reducción, por tanto, de las restricciones actuales que limitan la libertad de usuarios y productores.[15] Esto ha de obligar a la remodelación del monopolio existente en las telecomunicaciones, al igual que ha de suceder en otros campos, como, por ejemplo, el energético. [16] Se trata, en definitiva, de suprimir los obstáculos derivados de la configuración de estas actividades como servicio público y su consustancial régimen de monopolio, a fin de conseguir la efectiva integración europea.[17] Y es que la apertura a la concurrencia en este sector deviene imprescindible, tanto por la presión de las empresas que reclaman una mayor liberalización y el derecho de acceso a un mercado en espectacular crecimiento, como por la internacionalización creciente del mercado y de sus redes de distribución (cabría incluso hablar de mundialización), que vuelven caduca la idea del proteccionismo y del aislacionismo estatal. Resulta por ello necesaria una desreglamentación del sector, que facilite la consecución del objetivo final de un mercado único, así como una adaptación de la estructura monopolística actualmente existente en España.[18]

REFERENCIAS BIBLIOGRAFICAS.

–ARIÑO ORTIZ, «La empresa pública», en vol. col. El modelo económico en la Constitución española, *Instituto de Estudios Económicos*, Madrid, 1981, p. 112.

–COCKBORNE, «La libéralisation du marché communautaire de L'Electricité: les telecoms montrent-ils la voie», *Revue de Droit des Affaires Internationales* núm. 7, 1990, pp. 851 y ss.

–CORTINA NAVARRO Y DE CARLOS BELTRÁN, «Telecomunicaciones y derecho comunitario», Noticias CEE núm. 84, 1992, pp. 20-26.

–CHEVALIER, «Les enjeux juridiques: l'adaptation du service public des télécommunications», *Revue Française d'Administration Publique* núm. 52, 1990, pp. 601 y ss.

–CHEVALIER, «La réglémentation des télecommunications», *Actualité Juridique. Droit Administratif* n.º 3 de 1991, pp. 203 y ss.

(14) En este sentido, (J.P. JACQUE, 1989).

(15) Sobre el coste-beneficio de la liberalización en el sector de las telecomunicaciones puede consultarse el documento de la COMISION «1992»: la nouvelle économie européenne», en Economie Européenne núm. 35 (monográfico), 1988, pp. 105-107.

(16) Sobre esta cuestión resulta interesante el trabajo de (J.E. COCKBORNE, 1990).

(17) (stoffaes, 1988).

(18) (J. CHEVALIER, 1990). Con todo, como bien apunta este autor, todos estos cambios aconsejan una redefinición de la noción de servicio público, inadecuada en el nuevo contexto comunitarios. Apuntamos simplemente la cuestión por exceder del ámbito de este trabajo.

–DÍEZ MORENO, «Las dificultades de la incorporación al ordenamiento español de las Directivas comunitarias sobre contratación en los sectores excluidos», *Noticias CEE* núm. 71, 1990, pp. 49-63.

–DELORS, «Orientamenti e indirizzi comunitari», *Il Diritto dell'Economia* núm. 1 de 1990, p. 9.

–GEBHARDT, «Reglamentación de las comunicaciones por satélite en los Estados miembros de la CEE», *Boletín de Telecomunicaciones*, 1991, núm. IV, pp. 223-231.

–GLAESNER, «L'article 100A: un nuovel instrument pour la realisation du marché commun», *Cahiers de Droit Européennne* núm. 5-6, 1989, pp. 615-626.

–JACQUE, «La communautarisation des politiques nationales», *Revue Française d'Etudes Constitutionnelles et Politiques* núm. 48, 1989, p. 30.

–MATTERA, El Mercado Unico Europeo. Sus reglas, su funcionamiento, Civitas, trad. esp., Madrid, 1991, p. 386

–MARTÍN MATEO, Liberalización de la Economía. Más Estado y menos Administración, Trivium, Madrid, 1988, p. 18.

–SAMANIEGO BORDIU, «La normativa comunitaria de los contratos de las empresas que actuán en los sectores del agua, la energía, los transportes y las telecomunicaciones», *Revista Española de Derecho Administrativo* núm. 71, 1991, pp. 357-374.

–SANTIAS VIADA, SANTAMARÍA DE PAREDES y LÓPEZ BLANCO, «El Derecho comunitario de la contratación pública», *Escuela de Hacienda Pública*, Madrid, 1991, pp. 52-60.

–SCHULTE-BRAUCKS, «Lévolution des Télécommunications dans le perspective du marché intérieur de 1992», la *Revue du Droit des PTT* núm. 19, 1990, pp. 3-6

–STOFFAES, «Transports, énergie, communications: lintégration des grands réseaus de services publics dans le cadre européen», *Problémes economiques* núm. 2097, 1988, pp. 16-19.

EDI: Desafío de una nueva práctica

AUDILIO GONZALES AGUILAR

Abogado. Universidad Externado de Colombia
Diplomado de Estudios especializados en Informática Jurídica y Derecho Informático de la Univ. de Montpellier. (Francia)
Miembro del equipo de ayuda del doctorado de Informática Jurídica de la Universidad de Montpellier
Investigador en Informática Jurídica
Asesor en la concepción de Sistemas de Ayuda a la Decisión en Derecho
(FRANCIA)

SECCION I. EN DERECHO PRIVADO

El Derecho frente a la nuevas tecnologías no se ha quedado al margen. La Informática no solamente sirve a la gestión de grandes bases documentales o interviene en las tareas cotidianas del jurista, sino que ella conduce a la transformación de las relaciones jurídicas. Ejemplo de esta nueva concepción de relaciones son los E.D.I... (del inglés Electronic Data Interchange o T.E.D. del francés Transfert Electronique des Données).

Los E.D.I. son el resultado de la fusión de la informática y la nuevas técnicas de telecomunicación que permiten reemplazar el documento papel en las transacciones comerciales a nivel internacional. En este estudio hemos constatado que el documento escrito es preeminente, y hace difícil la aceptación de la Nuevas Tecnologías de la Información, de una parte, a causa de la seguridad de los datos transmitidos y de otra parte, por la desconfianza frente a estos nuevos procedimientos de transmisión de la información.

Los E.D.I. van a transformar las relaciones comerciales internacionales. «Actualmente el número de organismos que utilizan en Europa la transferencia electrónica de datos (T.E.D.) dobla cada año. Este rápido crecimiento, estos últimos años, pone en evidencia la necesidad de aprovechar este tipo de comercio y encontrar soluciones comunes a ciertos problemas que se plantean a nivel europeo»[1]

1. Los E.D.I. y la prueba

Las transacciones internacionales se fundamentan en la utilización del documento escrito. Se estima alrededor del 7,5%, en promedio, el costo del trabajo-documento papel en relación al costo de la mercancía sobre un total de 1900 millones de dólares por año. En Francia, más de diez millones de documentos originales son emitidos por las empresas francesas en dirección a treinta y nueve millones de destinatarios.

A menudo, las mercancías se desplazan mas rápido que los documentos, en gran parte, por el hecho de que los envíos por el correo postal y el registro de datos implican, una pérdida de tiempo. La circulación de datos conducen a una aceleración de las transacciones.

En efecto, los E.D.I.. desarrollan una nueva práctica que transforma el sistema clásico de transacciones por documento escrito. Esta transformación se traduce en el campo jurídico, más exactamente sobre el terreno del Derecho probatorio. Según el tablero anexo (ver infra Sección II), la mayor parte de los estados europeos exigen aún la firma manuscrita en las facturas comerciales. De otra parte, los soportes y los registros electrónicos e informáticos no son totalmente admitidos y no teniendo un valor probatorio asegurado en los regímenes existentes. [2]

En nuestro trabajo haremos primero una aproximación desde el punto de vista teórico de los E.D.I... (I) y luego, una referencia a las aplicaciones de los E.D.I... en los países de la C.E.E. (II).

I. Aspectos teóricos de los E.D.I...

Las E.D.I.. o Transferencia Electrónica de Datos Informatizados, «consiste en el intercambio o transferencia de datos preparados o formateados de manera standard entre las diferentes aplicaciones que funcionan en los ordenadores de asociados comerciales con un mínimo de intervención manual.[3]

---

[1] Commission des cummunautés Européennes, D.G. Télécommunications industries de l'infirmation et innovation, FR/89/1, EUR 122293

[2] Le rapport de communautés Européennes (Commission des Communautés Européennes, D.G. Télécommunications industries de l'infirmation et innovation, FR/89/1, EUR 122293) precisa que si «la TED busca, a término, la supresión del soporte papel y de las firmas, el derecho nacional o internacional, la práctica exige a menudo, documentos escritos acompañados de una firma manuscrita, que se justifica en las declaraciones de aduana, contables, fiscales y administrativas, o en todo documento que pueda servir de prueba o de base a una negociación».

[3] *Aspects de l'E.D.I. (Electronic Data Interchange),* Commission des Communautés Européennes, D.G. Télécommunications industries de l'infirmation et innovation, FR/89/1, EUR 11883 FR, p. 12

Esta definición general puede aplicarse a cualquier aplicación informática o telemática.

En un primer momento, los E.D.I... se definieron como la «transferencia electrónica de documentos», queriendo designar con esto la transferencia de documentos comerciales (facturas, pedidos, etc.). Posteriormente se pasó de la noción de Transferencia electrónica de documentos a un concepto más general de «*Transferencia de datos informatizados*».[4]

Los E.D.I.. se distinguen por dos características principalmente: la primera, implican una estructuración normalizada de la información, que no poseen los otros medios de transmisión y en segundo lugar, los E.D.I... ponen en relación los sistemas informáticos de empresas diferentes. Es por este segundo aspecto que pensamos que los E.D.I... pueden analizarse desde el punto de vista de la normalización.

A. El comercio Internacional y los E.D.I.

Actualmente la mayoría de empresas utilizan las ventajas ofrecidas por la informática: las redes de transmisión de datos han automatizado la circulación interna de la información (todos los documentos comerciales, facturas, pedidos son realizados por ordenador). De esta ventaja sólo saca provecho la empresa que transmite los documentos emitidos por un centro informático, ya que estos mismos datos son tratados por medios informáticos por los destinatarios exteriores de la información. Los americanos llaman a este proceso la «second hand information».[5]

Para el éxito del E.D.I.., dos condiciones se hacen necesarias: la primera, que la empresa posea un equipo físico de comunicación, es decir, una red de transmisión de datos adaptada y compatible (sistema abierto), para transmitir correctamente los datos. La segunda condición es el empleo de un lenguaje universal, constituido de una sintaxis y un vocabulario comunes. La ausencia de uno de estos elementos hace que el sistema de E.D.I.. reemplace «la montaña de papel por una Torre de Babel electrónica bastante costosa e incoherente.» [6]

Los E.D.I.. son aplicables al comercio, el transporte y la administración. En todos esos casos concretos de aplicación los E.D.I... no tiene fronteras y está al alcance de toda empresa [7].

---

[4] M. Nouvion et A. Gheysen, *EDI: un Esperanto poru décloisonner l'informatique,* in France Télécom, aôut 1988, p.22 et s.

[5] El nuevo tratamiento de los documentos es la fuente de numerosos errores y casi todos los documentos así tratados contienen datos erróneos. «Información de segunda mano».

[6] M. Nouvion et A. Gheysen, *EDI: un Esperanto poru décloisonner l'informatique, en* France Télécom, aôut 1988, p. 24 y ss.

[7]10 Los EE.UU. han entrado con antelación en este nuevo mercado: E.D.I. se extiende como una mancha de aceite. El 53% de las innumerables grandes empresas están dotadas de la red E.D.I. En Europa, son los países anglosajones los que están más avanzados. Francia tiene retraso: ha sido solamente en 1987 cuando ha emprendido la operación marketing y las empresas no tienen confianza, ni siquiera, en sus propios equipos informáticos. El fantasma del papel está presente en todas las actividades. Comprendidas la actividad y la reflexión jurídicas.

Sólo será necesario tener un ordenador, un equipo de telecomunicaciones (una línea de telefónica y un modem). Para tener una visión general de los E.D.I..., analizaremos en un primer momento la normalización (1) y luego, en un segundo tiempo, la estructuración de los datos (2).

B. La normalización.

El diálogo entre las empresas requiere que ellas lleguen al menos a «entenderse» desde un punto de vista informático. Este proceso lo llamaremos normalización. Entendemos por normalización documental, la unificación del vocabulario y de la sintaxis del mensaje a transmitir. La automatización del mensaje del documento comercial a transmitir se hace a partir de la normalización documental. Esta tarea, según el informe de las Comunidades Europeas, es de imperiosa necesidad: «Los E.D.I.. y la normalización son indisociables. Como en el mismo caso de una lengua, las normas los E.D.I.. se componen de una gramática (sintaxis, reglas de estructuración de los términos de los datos a transmitir...), así como de un glosario de términos (repertorio de los términos de la información transmitida, de los segmentos y de los mensajes» [8]

Es en los Estados Unidos donde comienza la normalización para el sector de los transportes en 1968. Pero fue solamente en 1985 cuando la American National Standards Institute (ANSI) [9] creó y estableció el formato X12. Por su parte, la Comisión Económica Europea de Naciones (UNECE) publicó en marzo de 1985 el repertorio de términos y elementos de los datos y mensajes comerciales. Y es en este momento cuando aparece el interés económico de los E.D.I... : ¡Los Estados Unidos controlan la mitad del mercado mundial.

Fue necesario esperar hasta 1986 para ver que los americanos y europeos se pusieran de acuerdo para elaborar un lenguaje común, elaborado por el grupo UN-JEDI (United Nation's Joint EDI Committee). El resultado de este trabajo fue el lenguaje TEDIFACT «Echange de données informatisées pour l'administration, le commerce et le transport».(de Transmisión de Datos Informatizados en la Administración, el Comercio y el Transporte TEDIFACT). A partir de ese lenguaje la Comisión Económica Europea desarrolla el programa para la Transferencia Electrónica de Datos Comerciales, TEDIS.

II. El lenguaje EDIFACT.

EDIFACT (Electronic Data Interchange For Administration Commerce and Transport) consiste en «un conjunto coherente de principios y definiciones para permitir la comunicación de datos administrativos, comerciales o logísticos, cualesquiera sea el equipo informático de los actores del intercambio de información y a través de todas las redes de telecomunicación» [10].

---

[8] *Aspects de l'E.D.I. (Electronic Data Interchange), Commission des Communautés Européennes, D.G. Télécommunications* industries de l'infirmation et innovation, FR/89/1, EUR 11883 FR.

[9] Instituto Nacioinal Americano de Normalización.

[10] Th. Piette–Coudol, *Contribution `a l'élaboration d'un régime juridique pour les*

De esta manera el EDIFACT se constituye en un lenguaje que define las reglas de transferencia de datos informatizados para la administración, el comercio y el transporte a nivel mundial [11].

Estas normas básicas permitirán a los E.D.I... desarrollarse dentro del campo internacional y, de satisfacer las necesidades de los usuarios, no importa cual sea el sector o el país. La oficina EDIFACT Board está compuesta de delegados de 18 países europeos así como de representantes de los organismos internacionales interesados por los E.D.I...

El lenguaje EDIFACT está orientado hacia el contenido de los documentos. Es una norma-lenguaje que permite armonizar y estandarizar los documentos comerciales. Este lenguaje está compuesto de: un vocabulario, una gramática, directivas para la concepción de mensajes estándares, la gestión de la segmentación del mensaje y los mensajes estandar. Este lenguaje está en conformidad con el modelo OSI, norma ISO 7496. Ventajas: la información es identificable, repertoriada y editada en todo momento y en todo punto de la cadena de la teletransmisión [12].

Para mayor comprensión de este lenguaje desarrollaremos, de manera sucinta la formación de los mensajes y la normalización EDIFACT :

A. Los mensajes EDIFACT.–

Encontramos del más simple, al más complejo:

1. Los términos básicos del dato.

Es, como su nombre lo indica, la unidad mínima de información empleada para la construcción de los mensajes de E.D.I.. estandard.

2. Los segmentos.

Es el conjunto de términos del dato unidos de manera funcional. Por ejemplo: nombre, dirección, encabezado y final del mensaje a transmitir.

3. Los mensajes.

Es el reagrupamiento de la serie de segmentos agenciados conforme a las reglas de la sintaxis establecida por el lenguaje. Se trata de mensajes estándares que cumplen las condiciones comerciales específicas como la facturación, el envío de órdenes de pedidos, las declaraciones de aduana, etc. [13]

B. Las normas del EDIFACT.–

Dentro de las principales normas podemos distinguir:

échanges de documents informatisés (E.D.I.), in Cahiers Lamy du droit de l'informatique, D, 1989, p.19

[11] Existe también la norma O.D.A. (office Document Arcitecture), aprobada en 1988 (ISO 8613). Ver Le Monde Informatique du Décembre 1988.

[12] Th. Piette–Coudol, *Contribution à l'élaboration d'un régime juridique pour les échanges de documents informatisés (E.D.I.),* en Cahiers Lamy du droit de l'informatique, D, 1989, p.21

[13] M. Marchand, *L'EDI,*Afnor-Edifrance, 1990 p.2

1. El vocabulario,

Está constituido por el repertorio de términos comerciales de Naciones Unidas (ISO 7372). Se trata de elementos de construcción y de definición de mensajes de EDI estándares.

2. La gramática.

Está conformada por las reglas de sintaxis del lenguaje EDIFACT de Naciones Unidas (ISO 9735): ellas permiten organizar de manera racional un fichero informático destinado a ser transmitido. Ellas fueron, igualmente adoptadas, por el CEN (Comité Europeo de Normalización), bajo la norma EN 29735.

3. El soporte.

La fórmula–marco para los documentos comerciales es la norma ISO 6422, utilizada principalmente para la concepción de mensajes, para la visualización sobre la pantalla y para la impresión del mensaje a través de la impresora.

Existen además diversos instrumentos que completan la tarea del lenguaje EDIFACT: diccionarios, directivas, notas explicativas y los códigos aprobados a escala internacional concernientes a los países, las monedas, las condiciones de entrega, pago y modos de transporte de las mercancías.

2. El programa TEDIS

La C.E.E. creó el programa T.E.D.I.S. (Trade Electronic Data Interchange Systems) buscando reagrupar los organismos relacionados con los E.D.I.. y, a su vez, mejorar la infraestructura europea de telecomunicaciones y desarrollar las medidas de seguridad, en armonía con las diferentes legislaciones nacionales en la materia.

I. Objetivos.

El programa T.E.D.I.S. está encargado de desarrollar a nivel europeo los principales componentes de los E.D.I.. Dentro de esos objetivos encontramos los siguientes:

a) Promover el tratamiento electrónico de los documentos comerciales que respondan a las normas internacionales y europeas reorganizadas en el lenguaje EDIFACT.

b) Estimular la industria europea de equipos y de servicios telemáticos, al objeto que pueda responder a la demanda del mercado internacional.

c) Evitar la proliferación de redes de transferencia electrónica evitando la generalización de la incompatibilidad de sistemas, sosteniendo y aconsejando la utilización común de normas internacionales de la C.E.E-O.N.U.

d) Buscar soluciones a los problemas jurídicos que podrían frenar el desarrollo de la transferencia electrónica de datos de uso comercial, y velar porque esas reglamentaciones restrictivas en materia de telecomunicaciones no se constituyan en obstáculos al desarrollo de la transferencia electrónica de datos de uso comercial.

e) Estudiar las necesidades de los sistemas de transferencia electrónica de datos comerciales en materia de seguridad con el fin de asegurar la confidencialidad de los mensajes transmitidos.

Para cumplir con estos objetivos, el programa deberá:

a) Tener en cuenta las necesidades específicas de la transferencia electrónica de datos, para desarrollar las políticas adecuadas en materia de telecomunicaciones y de normalización.

b) Establecer una concertación estrecha con la industria de materiales y equipos y las empresas y servicios finales a los usuarios.

c) Asegurar una acción común sobre la normalización, la tarificación, el multilingüísmo, la confidencialidad, la seguridad, etc. (acción horizontal) con los proyectos pilotos existentes en Europa (acción vertical).

A. La estructuración de los E.D.I.

Las normas TEDIFACT se interesan, no solamente de la forma de los datos transferidos electrónicamente, sino también de su contenido. Es por eso que, referido a la empresa la utilización de la transferencia electrónica de datos no podrá desarrollarse sino a condición de efectuar una concertación entre los actores privados y las administraciones responsables de las telecomunicaciones.

La selección va a depender de las necesidades de cada uno de los diferentes interesados comerciales. Esto es posible gracias al trabajo de la oficina de TEDIFACT Board, comisión encargada de verificar la conformidad con las normas internacionales para la transferencia electrónica de datos con los transportadores, la aduanas y la banca.

Los mensajes E.D.I. destinados a las transacciones comerciales tienen la misma estructura que los documentos escritos.

Los mensajes E.D.I. recogen todos los documentos necesarios para el intercambio comercial. Ellos son preparados por TEDIFACT Board y serán publicados bajo la forma de recomendación por O.N.U. Entre los diversos documentos en fase final, encontramos las facturas, las órdenes de compra, las declaraciones de aduana y las órdenes de transporte.

En el marco de una transacción comercial, según la concepción de los E.D.I.., fue necesario tener en cuenta, de una parte, todos los actores de la negociación y, de otra parte, la formación y la ejecución del contrato. Intentaremos describir de manera suscinta una transacción realizada por los E.D.I.

1. La formación del contrato.

En las relaciones comprador/vendedor-distribuidor, la transferencia electrónica debe tener en cuenta los siguientes aspectos:

a) *La proposición:* El comprador hace un pedido o el vendedor responde a una oferta hecha al comprador señalando los precios, la fecha y la condiciones de entrega. Un mensaje E.D.I. debe incluir: las partes implicadas,

los productos solicitados, las cantidades, la fecha de disponibilidad y entrega, el transporte y el lugar de la entrega de las mercaderías.

b) Sobre la base de ese pedido o esa proposición hecha por el comprador y vendedor, respectivamente, se llegará a la conclusión del contrato y a emitir una orden por cada una de las partes.

2. Ejecución del contrato.

El tipo exacto de mensaje entre el comprador y el vendedor depende de los acuerdos comerciales celebrados previamente. Podemos señalar entre los más importantes los siguientes:

a. Las instrucciones de entrega.–

Consiste en un mensaje simple que describe las mercaderías a entregar y que permite al distribuidor planificar su producción y cumplir los plazos previstos de entrega. En respuesta al vendedor, envía una *confirmación o una modificación.* [14]

b. El aviso de expedición.–

El remitente/vendedor envía el mensaje de aviso de expedición en el que precisa los productos, las cantidades y el modo de transporte.

c. Los pagos.–

Un mensaje obligatorio es la factura, por la cual el vendedor precisa en detalle las mercaderías, los servicios prestados, las cantidades, el precio, las condiciones de pago, etc.. Con la utilización de los E.D.I.. se puede igualmente enviar un estado de cuentas y en caso de error, las *notas de débito o de crédito.*

Igualmente las empresas pueden procesar sus cuentas, enviando *la orden de pago al banco*. En los bancos, los soportes magnéticos y la teletransmisión inspiran confianza y responden a las exigencias de eficiencia y rapidez.[15]

d. Orden de transporte.–

En esta parte de la transacción un tercer actor aparece: el transportador. Los mensaje que resultan de esta fase sirven para la reserva provisional de un servicio de transporte, la confirmación, la factura por los gastos de transporte y la orden de pago dirigida al banco.

e. Formalidades de aduana.–

Si la transacción es efectuada a nivel internacional, se hace necesario una serie de trámites administrativos ante las autoridades aduaneras. Así encontramos un cuarto actor en la transacción comercial: «*El exportador y el importador o sus agentes someterán su declaración de aduana* al tratamiento

---

[14] El sector automotor tomó la iniciativa, en un esfuerzo de cooperación con los distribuidores, de normalizar los mensajes en sus transacciones comerciales. En Europa existe el proyecto Odette sobre este sector, Ver W. Sciarone, algunas reflexiones sobre una práctica, en Las transacciones internacionales asistidas por ordenador, litec, 1987, p. 31

[15] J. Réga, *La práctica de las transacciones internacionales asistidas por ordenador y los servicios, en Las transaciones interrnacionales asistidas por ordenador*, Litec 1987, p. 39

de un mensaje E.D.I., precisando las partes e indicando en detalle y con precisión, las mercaderías y productos, el medio de transporte y su embalaje, los gastos de importación o exportación, y la licencia de importación o exportación» [16]

B. Las redes de telecomunicación.–

Una vez analizada la estructuración de los datos, nos queda por ver el modo de trasmisión de los datos procedentes de una empresa que quiere utilizar los E.D.I... En el contexto, se hace necesario referirnos a las redes de telecomunicación que hacen parte integrante del funcionamiento de los E.D.I. [17]

Dentro de las posibilidades para crear un sistema de E.D.I. podemos encontrar :

1. El acceso directo.–

La primera manera de abordar los E.D.I. es el llamado *acceso directo*, es decir, que los corresponsales utilicen sus propias líneas telefónicas y sus propios modems. La ventajas de este sistema son la simplicidad, la utilización de sus propias líneas telefónicas (red telefónica conmutada RTC) y la mínima inversión en equipos y programas de transmisión.

The quick brown fox jumps over the lazy dog. Now is the time for all men.

Inconvenientes:

a) El teléfono no fue concebido para la transmisión de datos, y la velocidad de esta operación depende de la utilización de líneas especializadas.

b) La existencia de problemas de seguridad en la transmisión de la información.

2. Redes de datos públicas.–

Se trata de redes de servicio nacional o internacional ofrecidos por la Administración de Correos y de Telecomunicaciones de casi todos los países. El usuario establece una conexión y transmite los datos al destinatario seleccionado. La transmisión de datos y la seguridad de los datos son asegurados por el responsable de la red. El costo de la transacción es facturado directamente por la Administración, sobre la base de la duración de la conexión a la red y al volumen de los datos transmitidos.

La red pública puede ser de acceso directo, o por comunicación por paquetes (caso de TRANSPAC). Puede tratarse igualmente de una *Red Numé-*

[16] *Aspects de l'E.D.I. (Electronic Data Interchange), Commission des Communautés Européennes,* D.G. Télécommunications industries de l'infirmation et innovation, FR/89/1, EUR 11883 FR.

[17] Es importante destacar que los métodos de transmisión de datos y sus protocolos se encuentran más allá de la esfera prevista en los normas de E.D.I. que sólo se ocupan de la adecuación formal de los datos que contienen este tipo de mensajes.

rica de Integración de Servicios, RNIS [18], bautizada NUMERIS por Télécom–Francia, su explotante. La RNIS permite la transmisión de mensajes, conversaciones, datos, textos e imágenes. Esta red está ofrecida a las empresas y a los usuarios profesionales. Entre 1991 y 1993 todos los países de las Comunidades Económicas Europeas estarán dotados de la RNIS. Los Estados Unidos comercializan esta red desde 1988.

3. Las redes de valor agregado.–

Son redes de transmisión creadas por particulares que arriendan a terceros, con el objeto de prestar un servicio a un grupo de usuarios abonados previamente. Estas redes pueden ser destinadas a asegurar las necesidades de un sector profesional específico (caso de S.W.I.F.T., red internacional de transmisión de datos bancarios).

Este sistema presenta las ventajas siguientes:

a) transparencia sobre la red de transmisión.

b) Facilidad de acceso a la red, especialmente al momento de la recepción de datos.

c) La existencia de una extensa gama de servicios.

d) Asesoría y consejo a los usuarios en todo punto de la red

e) Seguridad del contenido y de la transmisión de los datos.

Un solo inconveniente: el costo elevado del servicio. [19]

4. Redes privadas.–

Es el caso de la empresa que crea su propia red de comunicación y la pone al servicio de sus asociados comerciales. Las grandes multinacionales han preferido este sistema, que les da el máximo de seguridad y confidencialidad de los datos transmitidos. El costo de estas redes privadas está en relación directa con el precio de las líneas de comunicación. Ejemplos de este tipo de redes son las redes de la General Motors y de Phillips.

II. Los E.D.I.: Aspectos jurídicos.

La «Transmisión de Datos Informatizados» E.D.I. permite intercambiar mensajes normalizados en lugar de documentos comerciales por escrito. No debemos olvidar que el escrito juega un rol importante en las transacciones comerciales: él satisface las condiciones de validez o de negociabilidad del acto jurídico en el mismo, y además es indispensable por razones contables, fiscales y, sobre todo, para responder a las necesidades de la prueba. [20]

---

[18] *Le RNIS Universal,* en 01 informatique, dossier spécial, núm. 1077, septiembre 1989.

[19] M. Nouvion et A. Gheysen, *EDI: un Esperanto pour décloisonner l'informatique,* in France Télécom, août 1988, p. 25

[20] Ver estudio de las Comunidades Europeas sobre los problemas técnicos y jurídicos de la T.E.D.I. en el que se hace un estudio del régimen jurídico en el campo comercial, fiscal y probatorio, con el fin de establecer los diferentes obstáculos encontrados en cada una de las legislaciones de los países miembros de las C.E.E.

En efecto, el E.D.I.. «en consecuencia suprime todos los documentos escritos que hasta el momento podían servir de prueba en caso de litigio o en el proceso». [21]

Los problemas jurídicos planteados por la transferencia electrónica de datos E.D.I. están unidos, de una parte, a la formación del contrato y a la desmaterialización de los documentos (A) y, de otra parte, a los problemas de prueba (B).

A. La desmaterialización de los documentos

La utilización de la transferencia electrónica de datos conduce a la desaparición del documento-papel dentro del marco de las transacciones comerciales. En las transacciones sin papel («paperless») podemos entrever diversos problemas relativos a la utilización de nuevas tecnologías, ya sea con respecto a la formación del contrato, ya sea con relación a la conservación y a la seguridad de los documentos informatizados.

1. Problemas jurídicos debidos a la tecnología.–

Estos problemas pueden producirse por diversas razones:

1) *Errores de origen técnico, como por ejemplo el mal funcionamiento del material informático o de los programas del ordenador o incluso de la red de transmisión.*

2) *Errores de origen externo,* debidos a las malas condiciones ambientales y atmosféricas que pueden provocar una avería en el sistema o alterar el mensaje transmitido.

3) *Errores de origen humano,* como por ejemplo la grabación errónea de datos luego de su codificación o decodificación o en la manipulación de los programas. En este caso, puede tratarse de la modificación, la destrucción o la apropiación fraudulenta del mensaje.

2. Problemas jurídicos en la formación y la ejecución del contrato.–

La transferencia electrónica de datos no es aplicable a todos los contratos. En efecto, ciertos contratos para su validez exigen ciertas formalidades y condiciones específicas incompatibles con los E.D.I.. Es el caso de los contratos de venta inmobiliaria o del contrato de caución.

Pero referido a los contratos encontramos también el problema relacionado con la *determinación del momento* o del *lugar de formación del contrato* (aspectos que son de una importancia considerables en la determinación del Derecho aplicable y en la determinación de la jurisdicción competente del litigio).

Diferentes teorías han sido formuladas sobre la conclusión del contrato: la de la emisión (el contrato se considera concluido en el lugar y en el momento en que la aceptación de la oferta es expedida al oferente), o aquella de la recepción (el contrato se entiende concluido en el momento y el lugar

[21] F. Chamoux, *TEDIS-Legal Workshop,* Bruselas, junio 1989

en que el oferente recibe la aceptación de la oferta), o finalmente la del conocimiento o del conocimiento de la aceptación (el contrato se entiende concluido en el momento y el lugar donde el oferente toma conocimiento de la aceptación de su oferta) [22].

B. Los problemas de la prueba.–

Esta problemática está relacionada fundamentalmente con la preeminencia del escrito–papel como soporte de los documentos con valor jurídico. Los documentos necesarios en una transacción comercial en general, no tienen la restricción de ser redactados por escrito en un soporte papel.

Por otra parte, en Derecho comercial los contratos son de forma libre y de libre contenido, siempre y cuando respeten los principios generales de la materia. Esta libertad se extiende a los demás documentos comerciales (catálogos, facturas, órdenes de pedido, aviso y recibo de entrega) donde la libertad es total para redactar o no un escrito. [23]

No obstante la facilidad que aportan los E.D.I.. a las transacciones comerciales, estas técnicas encuentran por oposición una respuesta jurídica inadaptada a la evolución técnica «Los documentos de los E.D.I. no son diferentes de los demás documentos producidos por medios informáticos: ellos no tienen ningún valor jurídico» [24].

Así, el desarrollo de la transferencia electrónica de datos paga su tributo a la supremacía del valor probatorio del documento escrito.

La problemática de la prueba de los E.D.I. resulta en términos generales de:

a. La obligación de establecer, entregar, expedir o conservar documentos escritos firmados. Es el caso, por ejemplo, de las autoridades de aduanas, que exigen al menos una factura por escrito al momento de la declaración de aduanas.

b. La dificultad de constituir una prueba de los mensajes transmitidos, dada la fugacidad de su transmisión por vía electrónica [25]

La necesidad de constituir una prueba responde a las necesidades de procurarse una prueba para fines fiscales, contables y, de últimas, en caso de litigio.

c. La necesidad de conservar la prueba durante el término de caducidad

---

[22] Volveremos sobre este aspecto en el cuadro del análisis de las diferentes legislaciones de los países miembros de las C.E.E.

[23] Sobre las obligaciones legales de los documentos comerciales objeto de una T. E.D.I. ver Th. Piette-Coudol, *Contribution à l'élaboration d'un régime juridique pour les échanges de documents informatisés (E.D.I.),* in Cahiers Lamy du droit de l'informatique, D, 1989, p. 21

[24] *¿Los documentos sin prueba jurídica?,* Telematique magazine, mars 1989, p. 49

[25] Actualmente las soluciones técnicas son diversas: cartas magnéticas, código de acceso, firma electronica etc.

y prescripción de las acciones procesales, o durante el período legal de un control fiscal o administrativo.

d. La necesidad de una seguridad jurídica [26], principalmente sobre:

1) La identificación de las partes, que puede ser asegurada por el responsable del sistema o por un tercero que pueda autenticar o certificar esta identificación.

2) El contenido del mensaje o de la orden recibida por el destinatario, que debe ser conforme a aquélla que fue el objeto de la transferencia por vía electrónica.

[26] Ver F. Chamoux, *TEDIS-Legal Workshop,* Bruselas, junio 1989

Flujo internacional de información

JORGE PÁEZ MAÑA
Doctor en Derecho
Coordinador de documentación científica del Consejo Superior de Investigaciones Científicas de España

LDA. EVA TRIVIÑO ACUÑA
Licenciada en Derecho
Profesional Autónoma
(ESPAÑA)

Una de las características de la actual situación socioeconómica de la humanidad es la consolidación de mercado internacional de bienes de información (fruto de la denominada explosión de los recursos automatizados de información) y la consiguiente comercialización de dichos recursos, generados para satisfacer las necesidades del desarrollo industrial, provocando la producción, almacenamiento y transmisión de este tipo específico de información (PELOU et VILLEUMIN, 1987).

El nuevo orden económico mundial, basado en la libertad de comercio, que permite la rentabilización de cualquier tipo de bienes susceptibles de ser objeto de tráfico mercantil en el mercado internacional (a tenor de las leyes de la oferta y la demanda), ha puesto de manifiesto, con el progresivo incremento del volumen de contratación de bienes de la información, el valor intrínseco de la misma.

La aplicación de las nuevas tecnologías al sector de la industria de la información ha revolucionado la estructura del mismo eliminando las barreras físicas espaciales provocadas por la necesidad de almacenamiento de los bienes que van a ofertarse en el mercado (los nuevos soportes de discos ópticos permiten almacenar elevados volúmenes de información en reducidos soportes físicos), minimizando la incidencia de la diversificación de suministradores de información especializada relacionada con sectores específicos (el establecimiento de grandes distribuidores de la información automatizada conectados a las redes de telecomunicación ha reducido considerablemente los problemas provocados por dicha multiplicidad), ampliando la extensión de dichos mercados (la información automatizada, almacenada en cualquier punto conectado a las redes de transmisión de datos, tiene acceso directo a los mercados internacionales de la información automatizada) y reduciendo los plazos de entrega de los bienes de información a los consumidores (el plazo transcurrido desde el momento del almacenamiento de la información automatizada en una base de datos hasta su puesta a disposición para los usuarios situados ante cualquier terminal de ordenador, es casi imperceptible).

La telemática, nacida del encuentro entre la informática y la telecomunicación, ha abierto paso al flujo internacional de información producida por la industria de bases de datos permitiendo que amplios sectores sociales puedan tener acceso a las ingentes masas de datos ofertadas por los distribuidores de información automatizada, facilitando el incremento del conocimiento mundial, el acercamiento entre diferentes culturas y en suma el desarrollo integral de la humanidad.

En la regulación jurídica del flujo internacional de datos se estipulan diferentes aspectos, relacionados con el contenido de la información transmitida, que obligan a establecer una serie de delimitaciones previas a fin de analizar los conflictos originados por las diferentes elaboraciones doctrinales del estatuto y naturaleza jurídica de la información (DIAZ, 1992), que generan manifiestos antagonismos y múltiples puntos de fricción.

Las estipulaciones de los diferentes ordenamientos jurídicos aplicables a las condiciones y requisitos de emisión, tránsito y recepción de la información, y las condiciones contractuales establecidas para facilitar, fomentar y proteger el flujo internacional de la misma parten de las siguientes estimaciones:

a) La consideración de dicho flujo como una manifestación del tráfico mercantil de bienes aptos para el consumo, con una valoración meramente comercial, estableciendo un estatuto de la información en función de su conceptualización como objeto de dicho tráfico en el mercado internacional (BRIAT, 1988).

Esta concepción mercantilista de la información, ha ido progresivamente evolucionando pasando desde una primera consideración de la información

como objeto inapropiable y por tanto exento de protección jurídica, a la estipulación de una serie de derechos relacionados con la misma iniciados con el reconocimiento del derecho a comunicar o escenificar una obra al titular del papiro donde ésta se encontraba escrita (identificando el derecho de propiedad del soporte de la información con el de explotación de su contenido) y, progresivamente (en especial tras los cambios cualitativos producidos por la aparición de la imprenta y posteriormente por el establecimiento del Estado liberal), ampliando el concepto de propiedad intelectual otorgando una serie de derechos subjetivos sobre las obras a una multiplicidad de sujetos que detentaban diferentes derechos sobre las mismas (editores, autores y por último, en el momento actual, titulares de las bases de datos).

Hoy en día se observa que el incremento del tráfico mercantil de la información ha provocado un fuerte desarrollo normativo regulador del mismo con la finalidad de preservar la seguridad jurídica de los actos realizados en función de dicho tráfico (WARUSFEL, 1988) ampliando el ámbito de aplicación de los contratos de compraventa, suministro, préstamo, depósito, cesión de uso y arrendamiento, admitiendo como objeto de los mismos a los bienes inmateriales de información, y estableciendo unas singulares especificaciones en función de las particulares características de este tipo de bien.

Junto a las específicas características del desarrollo normativo hay que tener en cuenta que la transmisión internacional de este bien informativo, se encuadra en el marco más amplio de la libre circulación de mercancías (VIVANT, 1988), siéndole por tanto aplicable las regulaciones de los diferentes contratos internacionales de transporte de mercancías.

Esta aplicación de las diferentes modalidades de contratación internacional, permite acometer la resolución de los conflictos jurídicos planteados ante daños o perjuicios producidos en virtud de la ejecución de los citados contratos, pudiendo exigirse el saneamiento de la información defectuosa transmitida, la indemnización por los daños producidos por fallos en el transporte de la información y la responsabilidad civil o penal por perjuicios derivados de culpa, dolo o negligencia en el cesionario o en el transportista de la información (SUAREZ MARTINEZ, 1988).

A nivel internacional puede observarse el desarrollo de Convenios y Acuerdos internacionales que regulan las condiciones a que debe someterse el tráfico mercantil de determinadas obras (literarias, científicas y artísticas) (CATALA, 1983) enmarcando la protección de los derechos de explotación de las mismas entre los derechos de propiedad intelectual (Convenio de Berna para la Protección de obras literarias y artísticas, Convención Universal de Ginebra sobre Derechos de autor, Pacto Internacional de Derechos económicos sociales y culturales, Ley Tipo de Túnez sobre Derechos de autor, etc.).

A nivel nacional, esta tipología de obras protegidas se amplía en función de lo estipulado en los diferentes Ordenamientos jurídicos a una diversidad

de obras entre las que cabe destacar, por su incidencia especial en el flujo internacional de información automatizada, a las colecciones de obras, informaciones o datos de cualquier tipo que por su selección o características incorporen algún grado de originalidad, que confirman los fondos de las diferentes bases de datos.

b) La delimitación de la información como elemento básico del derecho a la información, entendido en sus dos facetas de derecho a informar y derecho a ser informado (Declaración Universal de Derechos humanos, Convenio Europeo para la Protección de derechos humanos y libertades públicas, Pacto Internacional de Derechos civiles y políticos, etc.).

Este derecho que ha sido recogido en múltiples textos constitucionales con la consideración de Derecho fundamental, parte de la concepción de la información como parte integrante de un fondo cultural de la humanidad en el que todos tienen el deber de verter sus conocimientos e ideas y, en contrapartida, del que todos pueden obtener la información que precisen para el libre desarrollo de su personalidad.

El derecho a la educación, el libre acceso a la cultura, la no discriminación por pensamientos, ideas o creencias, la libertad de opinión y el derecho a la libre investigación, son características de esta faceta que pretende potenciar el establecimiento de un patrimonio cultural de la humanidad sin limitación de fronteras, y su puesta a disposición del conjunto de personas y colectividades integradas en la misma, con la finalidad de hacer realidad el principio de igualdad de oportunidades a nivel internacional.

En el reconocimiento y aplicación del derecho a la información se enmarca la desregulación de la protección jurídica de las ideas, y su consideración como fruto y objeto de ese patrimonio cultural de la humanidad, la libre circulación de noticias sobre hechos o temas de actualidad, el paso al dominio público de las obras protegidas por la regulación de la propiedad intelectual transcurrido un determinado lapso de tiempo, la autorización de reproducción o traducción de algunas de dichas obras con fines de educación e investigación en determinadas circunstancias, y la obligatoriedad de depositar un determinado número de obras, previo a su distribución comercial, y el libre acceso a las mismas en determinadas bibliotecas o archivos de titularidad pública.

c) La concepción de la información como base de la intercomunicación personal, atendiendo a los aspectos del flujo internacional de información relacionados con la forma de trasmitir iniciativas, realizar transacciones comerciales, formalizar ofertas y demandas, realizar campañas publicitarias comerciales, llegar a acuerdos, acercar posiciones, fomentar colaboraciones, e incluso de ratificar formalmente acuerdos por vía telemática.

Esta faceta de la transmisión internacional de información, que progresivamente va ampliándose con la incorporación de nuevos elementos tecnológi-

cos que permiten eliminar barreras espaciales (audio, tele o videoconferencias con flujos de información interactivos) presenta unas características, ligadas a las necesidades socio-económicas de intercomunicación entre personas, que inciden en la regulación jurídica de las telecomunicaciones y en los aspectos relacionados con los denominados contratos informáticos.

d) La conveniencia de incluir, como parte fundamental del patrimonio universal de la humanidad, las normas emanadas del Derecho internacional y los dictámenes y resoluciones emitidas por los órganos e instituciones internacionales, a fin de dirigir la conformación de la conciencia universal estableciendo una serie de directrices con las que pretenden regular la convivencia internacional. Esta faceta similar a la provocada por los diferentes Ordenamientos jurídicos nacionales, obligando a dar publicidad a sus leyes y sentencias excluyéndolas expresamente como objeto de propiedad intelectual, tiene como finalidad el fomentar el conocimiento de las normas orientadoras o imperativas establecidas en dichos ordenamientos, a fin de obtener un consenso social sobre la conveniencia de aceptarlas como propias y de exigir su cumplimiento, lo que obliga a desproteger el valor mercantil que dichas obras podrían tener a fin de potenciar su más amplia difusión.

Asimismo la incidencia y repercusión de la realización o manifestación de determinados actos u opiniones por determinados órganos públicos o por personas que acaparan la atención de amplios sectores sociales permite, en función del interés de los propios autores sobre la amplia difusión de los mismos (informes oficiales, índices y estadísticas públicas, datos sociales, avisos de subvenciones y ayudas, información sobre política económica, etc.), del interés público y del ejercicio del libre derecho a la información, el paso al dominio público de la información recopilada sobre dichos eventos.

e) La necesidad de limitar el acceso y difusión de determinados tipos de información (excluidos por tanto del libre ejercicio del derecho a la información) que puedan suponer un peligro real para la seguridad del Estado, el orden y libertades públicas, la prevención, investigación o represión de delitos, el interés general de los pueblos, o para la dignidad, honor o imagen de personas individuales.

La difusión de algunos de estos tipos de información (información militar, secretos oficiales, materias reservadas, etc.) suele estar expresamente prohibida y exige la adopción de especiales medidas de seguridad sobre los archivos donde se encuentra e incluso sobre los lugares y condiciones de acceso en los que se encuentran ubicados los mismos, ante la necesidad de los diferentes Estados de autoprotegerse, y de proteger el orden público, la moral y el patrimonio histórico-cultural de sus pueblos.

Estas limitaciones de difusión de información interna que considere secreta e incluso de difusión de información de caracter científico o tecnológico a países sobre los que se pretende efectuar un bloqueo informativo, se encua-

dran, junto a la limitación de recepción de informaciones externas de determinadas características (incitación al terrorismo, propaganda ilícita, publicidad ideológica, etc.) en el marco de la utilización política de la información.

Asimismo hay que tener en cuenta que la transmisión internacional de informaciones ilícitas, falsas o fraudulentas agrava, precisamente en función del daño producido por el ámbito de difusión de dicha información, las penas tipificadas por la ejecución de dichos delitos.

f) La prevención de atentados contra la dignidad o vida privada de las personas mediante el acceso, recolección y tratamiento de sus datos nominativos.

Respecto a este tipo de información, diversos ordenamientos jurídicos han establecido una serie de limitaciones en previsión de que puedan establecerse previsibles pautas o perfiles de comportamiento de personas individualizadas, vulnerando los derechos a la intimidad de las mismas.

Estas especificaciones normativas, surgidas inicialmente de la sensibilización de determinadas colectividades ante la posibilidad de utilización de sus datos personales para finalidades diferentes a las que originaron su recolección, han ido progresivamente incidiendo en el desarrollo del Derecho internacional marcando unas pautas a seguir para la determinación del derecho individual a la privacidad.

Como principios básicos de la regulación del derecho a la protección de la privacidad de las personas ante el tratamiento o difusión de los datos que la conciernan podemos reseñar las siguientes (HEREDERO HIGUERAS, 1992):

–La especificación del ámbito subjetivo de la protección, que determinados ordenamientos limitan a las personas físicas, mientras otros extienden dicho ámbito acogiendo, junto a éstas, a las personas jurídicas.

–La exigencia de que las bases de datos donde se almacenen datos nominativos informen suficientemente sobre su existencia, exigiendo determinados ordenamientos que esta información se realice mediante la inscripción de la base en un Registro Oficial de bases de datos nominativas, reflejando en el asiento correspondiente el nombre y dirección de la base y del titular de la misma, la finalidad perseguida con su producción, los tipos de datos que se pretenden almacenar, y la posibilidad de efectuar cesiones de datos a terceros.

–La necesidad de crear un órgano independiente de control de este tipo de bases de datos, con autoridad para su supervisión y potestad para imponer sanciones administrativas o iniciar procedimientos jurisdiccionales por incumplimiento de las obligaciones legales que se imponen a los titulares de este tipo de bases de datos.

–La obligatoriedad de que la recogida de datos se realice con el consentimiento de los afectados cuando los datos no sean accesibles al público o con el correspondiente respaldo normativo, debiendo en ambos casos informar a

los interesados sobre la voluntariedad u obligatoriedad de suministrar los datos, sobre la titularidad de la base en la que van a ser almacenados, sobre su finalidad y sobre la posibilidad de que dichos datos puedan ser cedidos a terceros cuando así se haya previsto.

–El respeto de los derechos de las personas afectadas, salvo excepciones explícitamente reglamentadas, al acceso y comunicación de los datos almacenados que le conciernan, a la rectificación de los incorrectos o que hayan sufrido alguna modificación, y a la cancelación de los datos perjudiciales, en los casos de voluntariedad, o que hayan dejado de ser pertinentes en función de la finalidad de la base (PEREZ LUÑO, 1992).

–La prohibición de difusión de datos sensibles (origen racial, ideología, religión, creencias religiosas, vida sexual y salud) salvo consentimiento expreso del afectado o razones de bienestar público, seguridad del estado o persecución de delitos.

–La exigencia de contrastar la veracidad de los datos, su puesta al día, su rectificación o complementación cuando se detectasen como insuficientes o inexactos, y su cancelación cuando hubiesen dejado de ser pertinentes en función de la finalidad de la base en la que fueron almacenados.

–La necesidad de que se extremen las medidas de seguridad sobre los archivos donde se encontrasen almacenados los datos y sobre el acceso a los mismos a fin de evitar el acceso a los mismos por personas no autorizadas.

–La Prohibición de realizar cruces o tratamientos no previstos al determinar la finalidad de la base, en perjuicio de las personas afectadas, y de transmitir los datos a países que no cuenten al menos con una protección de los datos personales similar al del país emisor de los mismos.

–El seguimiento y control de las cesiones de datos a fin de informar a los cesionarios sobre las variaciones que se produzcan en los mismos.

–La explícita regulación normativa de las excepciones a estos principios para aquellos tipos de bases de datos que por su especialidad exijan un tratamiento diferenciado, con la especificación del alcance de las limitaciones y las formas de control respecto a su ajuste a la legalidad (bases de datos policiales, fiscales, militares, registrales, censales, estadísticas, de secretos oficiales o de servicios médicos o sanitarios).

Habida cuenta de la disparidad de ordenamientos jurídicos y que la diferente protección otorgada tendente a garantizar la intimidad personal ante tratamientos automatizados de datos personales, en la actualidad diversos Ordenamientos jurídicos prohiben taxativamente la transferencia de datos personales a terceros países que no proporcionen un equiparable nivel de protección a las personas concernidas, lo que ha provocado una serie de iniciativas a nivel internacional con objeto de homogeneizar el flujo internacional de datos personales (PÉREZ LUÑO, 1989).

Estas consideraciones obligan a acompasar el desarrollo normativo internacional y nacional del flujo internacional de información a las necesidades de protección del mercado internacional de la información y a las necesidades nacionales de acceso a la misma para lograr una mayor igualdad de oportunidades.

Esta doble perspectiva pone de manifiesto una de las principales circunstancias de desigualdad entre los países desarrollados y los países en desarrollo (desequilibrio norte-sur) configurando un doble orden mundial, el primero de los cuales aboga por una libertad de economía de mercado en el que uno de los bienes que se ofertan en el mismo es el de la información, mientras el segundo aboga por la limitación de dicha libertad en atención a la instauración del principio de igualdad de oportunidades, procurando de esta forma limitar su dependencia de los países mas desarrollados.

En esta disyuntiva se hace preciso moderar los deseos de mercantilización casi absoluta de los bienes informativos y sopesar las condiciones sociales que objetivamente permitan establecer limitaciones al citado comercio basadas en necesidades reales de desarrollo cultural o científico, a fin de coadyuvar al desarrollo armónico integral de la humanidad.

BIBLIOGRAFIA

BRIAT, M.: Information et flux transfrontieres de donnees, Brises, 12, novembre 1988, pp. 133-140.

CATALA, P.: «La propiete de l'information», Atti 3º Congresso internazionale sul tema L'informatica giuridica e le comunita nazionali ed internazionali, Roma, Mayo 1983, Sess. II, 23, pp. 126.

DÍAZ, F. E.: «Naturaleza jurídica de la información», Encuentros sobre Informática y Derecho 1990-1991, ed. Aranzadi, Pamplona 1992, pp. 35-51.

HEREDERO HIGUERAS, M.: «La protección de los datos personales registrados en soportes informáticos», Actualidad informática Aranzadi, 2, Enero 1992, pp. 1-3.

PELOU, P. et VUILLEMIN, A.: Innovation et nouvelles technologies de l'information, La Documentation française, París 1987.

PÉREZ LUÑO, A. E.: «Del habeas corpus al habeas data», Encuentros sobre Informática y Derecho 1990-1991, ed. Aranzadi, Pamplona 1992, pp. 171-179.

PÉREZ LUÑO, A. E.: «La incorporación del convenio europeo sobre la protección de datos personales al ordenamiento jurídico español», ICADE, Informática y Derecho, 1989, pp. 29-43.

SUÁREZ MARTÍNEZ, D. F.: «Responsabilidad de los productores de información automatizada frente a los usuarios», Actas del II Congreso Iberoame-

ricano de Informática y Documentación, Mar del plata, Argentina, diciembre 1988, pp. 621-626.

VIVANT, M.: Circulation de l'information et droit europeen, Brises, 12, novembre 1988, pp. 141-145.

WARUSFEL, B.: «Les flux transfrontieres de donnees en Europe. Aspects juridiques», Documentaliste, v. 25, nº 1, janvier-fevrier 1988, pp. 13-17.

Notas sobre las nuevas tecnologías de la información y sus relaciones con el derecho a la Comunicación

LUIS FERNANDO RAMOS SIMÓN

Licenciado en Derecho
Doctor en Ciencias de la Información
Técnico de la Dirección de Información y Comunicación Social de Unidad Eléctrica (UNESA)
Profesor asociado de Empresa
(ESPAÑA)

Vivimos en una fase de la civilización a la que se ha dado en llamar «sociedad de la información», expresión con la que se quiere significar el papel determinante que hoy en día tienen los medios y técnicas de información y comunicación. Sociedad de la información, sociedad postindustrial, sociedad digital son términos sinónimos que tratan de definir, con distintos matices, el nuevo modelo económico y social al que la sociedad actual se encamina, caracterizada por el papel determinante que están adquiriendo las nuevas tecnologías informativas (NTI). Estos nuevos productos de la revolución electrónica están caracterizados por su capacidad, que parece infinita, para contener información. Es este fenómeno de continuo progreso de las tecnologías informativas lo que ha creado esas expectativas de cambio social a cuya situación se le atribuyen las denominaciones referidas más arriba, aunque parece que es el término sociedad de la información el que cuenta con más adeptos.

Vaya por delante que no está todavía claro cuáles serán los usos sociales de esas nuevas técnicas, ni cómo van a influir en la vida cotidiana. A pesar

de la inminencia del advenimiento de esa nueva sociedad, no está claro cómo se desenvolverá la oferta técnico-mercantil, ni cómo afectará a las futuras formas de vida. Al hablar de la omnipresencia de los chips electrónicos en nuestra vida, los autores de «La Sociedad Digital» (Mercier, Plassard y Scardigli), advierten que «el único problema consiste en saber qué... «alma» les estamos dando». Hasta ahora, las nuevas tecnologías no han revolucionado el pensamiento, a lo sumo, han aportado velocidad a los procesos mecánicos. Desde el punto de vista político, las nuevas tecnologías aparecen asociadas a la libertad de opinión, a la libre circulación de información y a las nuevas formas de participación. Pero también aparecen relacionadas al reforzamiento de las tradicionales barreras de poder, a nuevas tecnologías impenetrables y a nuevas formas de control social centralizado y descentralizado (Burkert).

LA SOCIEDAD DE LA INFORMACION

Por otro lado, en esta nueva sociedad, la información en el marco de las nuevas tecnologías hace alusión a la capacidad de almacenamiento, transporte y tratamiento de los datos que son capaces de procesarse. Obsérvese que esta noción de información no tiene en cuenta la función social de los mensajes. Es información todo lo que puede ser objeto de un tratamiento numérico. De ahí que la reducción a información de todo dato transmisible por estas técnicas, da lugar a que se denominen tecnologías de la información.

¿Qué es la sociedad de la información? En primer lugar, es un crecimiento del sector cuaternario. A la tradicional división de los sectores de la economía –agricultura, industria y servicios– habrá de añadirse el de la información, el cual presenta la más fuerte expansión. Machlup es el primer autor que intenta describir el fenómeno. Según su trabajo, punto de referencia de muchos posteriores, en el año 1958, el 29% del producto nacional bruto estadounidense se derivaba de aquello que él define como la «industria del conocimiento». Porat, en un trabajo posterior, constata que las actividades ligadas directa o indirectamente con la información ocupan en 1970 al 50% de la fuerza de trabajo de Estados Unidos, frente al 30% en 1960.

Daniel Bell es otro de los más conocidos tratadistas que ha estudiado el fenómeno. Sostiene Bell que, si la sociedad industrial está basada en la tecnología mecánica, la sociedad postindustrial será modelada por una tecnología intelectual. Si el capital y el trabajo son las mayores características de la sociedad industrial, la información y el conocimiento lo son, en cambio, para la sociedad postindustrial. Para Bell, el saber de los comunicadores va a ser definitivo a la hora de decidir.

Richieri dice que la sociedad de la información trata de la producción, elaboración, circulación y consumo de gran cantidad de datos y de conocimiento (que abarca todos los campos de la actividad humana) relativos a

individuos, grupos y naciones, datos públicos y privados, económicos y científicos, políticos y militares.

EL DERECHO A LA COMUNICACION ANTE LOS NUEVOS FLUJOS INFORMATIVOS

Emitir y recibir mensajes es una exigencia de la vida en la sociedad. Esta actividad se pone en práctica mediante el despliegue de un conjunto de facultades que integran el contenido del derecho a la comunicación, al que podemos definir como «conjunto de facultades, inherentes al hombre como ser sociable, para intercambiar y poner en común diversas formas de mensaje» (Farias, 1991). Jean D'Arcy, fundador de Eurovisión en 1954, fue el primero en saludar el advenimiento de los medios posteriores a la televisión, considerándolos como una nueva opción para la libertad de expresión. En un artículo publicado en 1969 en la revista de la U.E.R. afirmó: «La Declaración Universal de los Derechos Humanos que hace veintiún años y por primera vez establecía en su artículo 19 el derecho a la información, algún día tendrá que reconocer un derecho de mayor alcance: el derecho del hombre a la comunicación» (Balle y Eymery, 1990). Este alegato en favor del nuevo derecho se articula en torno a dos argumentos principales: el primero reside en las virtualidades que entrañan las nuevas técnicas de comunicación; el segundo no es otro que la expresión renovada del viejo ideal de una sociedad de «comunicación», de una sociedad fraternal y solidaria, reconciliada consigo misma. La reciente evolución de los medios, suponía para Jean D'Arcy, que después de un largo periodo de comunicación unidireccional y vertical, ha llegado el momento de la comunicación interactiva y horizontal gracias a las nuevas técnicas.

Desde el punto de vista jurídico, afirma Farias que el derecho a la comunicación integra el derecho a la libertad de expresión de pensamiento, ideas y opiniones; al que posteriormente se incorpora la libertad de información.

En la fase actual, que tiene su inicio histórico en la Declaración Universal de Derechos Humanos de 1948, el derecho a la comunicación abarca un haz de facultades cuyo desarrollo impone al Estado una serie de obligaciones de signo contrario: positivo y negativo. Por un lado, la consideración del derecho a la comunicación como derecho de libertad, exige la abstención del Estado; y como derecho para promover y facilitar la participación, impone la prestación positiva por el Estado de ciertas actividades y servicios.

El reconocimiento normativo universal del derecho a la comunicación es preciso matizarlo en sus luces y en sus sombras. Dice Farias que sus luces proceden de la Declaración Universal y del sesgo positivo que la función del poder político toma en el Estado social de derecho, que proclama la promoción de los derechos fundamentales y la remoción de los obstáculos a su libre desarrollo (acceso a los archivos y oficinas de la administración y los relati-

vos al secreto). Las sombras del derecho a la comunicación son de origen político y económico. La sombra política, en el orden internacional, se manifiesta en la dificultad del individuo para acceder a las instancias jurisdiccionales de los organismos que lo han proclamado. En el orden político interno, las sombras proceden del desvío egoísta del Estado mediante la «extensión de los controles gubernamentales en los terrenos de la comunicación social». En el orden económico, la concentración económica de los medios de comunicar, dinamizada por el desarrollo tecnológico, tiende a «oligarquizar el ejercicio de las facultades del derecho», lo que desemboca en una censura material impuesta por el poder económico.

EL PAPEL DEL ESTADO

Hay coincidencia general en señalar que este caudal informativo, consistente en datos y cifras, no tiene ninguna relación directa en su contenido con la estructura política. Es decir, se trata de una información que no socaba los cimientos del Estado, ni amenaza a los Gobiernos. Por otro lado, esta información, generada por ordenadores u otros medios sofisticados, resulta muy costosa de conseguir y mantener. En la práctica, sólo las grandes corporaciones y el Estado disponen de recursos suficientes para recabar y gestionar ese ingente volumen de datos. Es, pues, una información de difícil acceso para el público general.

De otro lado, la información así entendida, requiere un soporte técnico complejo, lo que hace preciso un grado de conocimiento de cierto nivel. Cabe recordar aquí una de las críticas más frecuentes hacia la nuevas tecnologías. La que se refiere a la división que se establece entre los que encuentran la «faz amigable» de las nuevas tecnologías y la de quienes tropiezan con la «jungla tecnológica». Es el futuro en «rosa» y el futuro en «negro» del que hablan algunos autores (Balle y Eymery, 1990).

Además de este componente que, de forma genérica podríamos denominar educativo y que afecta al ejercicio del derecho a la comunicación, por cuanto vulnera el valor democrático de la igualdad; existe otro condicionante de la misma importancia: la capacidad económica para acceder a esa información, aspecto aludido también por Farias. No parece ahora que nos encontremos en una situación similar a la de la segunda mitad del siglo XIX, en la que el dinamismo de los empresarios de prensa, gracias principalmente a la publicidad, logró llevar la cultura a todas las capas sociales a través de los periódicos. De modo simultáneo, el Estado creó una red de bibliotecas y centros culturales donde los ciudadanos podían acceder de forma gratuita a toda clase de información y conocimiento. ¿Qué futuro presenta en este aspecto la difusión de los productos –caros– de las nuevas tecnologías?

Si se deja de un lado el porvenir que les espera a la prensa y a los medios audiovisuales clásicos, podemos centrarnos en cómo se financiarán

los grandes centros de información. Las futuras bibliotecas electrónicas, o como decidan llamarlas, se enfrentan a muchos interrogantes. En el supuesto de que el Estado asuma el coste de la información, la sociedad es cada vez más consciente de la valoración económica de ese servicio gratuito que presta y eso porque el coste de una consulta telemática se hace más perceptible que una consulta tradicional. De ahí que en los próximos años se planteen cuestiones tales como:

–¿Pagará el usuario los servicios que prestan las bibliotecas públicas? (algo impensable en la actualidad).

–¿Se establecerá una tasa de utilización por los servicios electrónicos y seguirá siendo gratuito el servicio tradicional, como los libros o documentos?

–Aún cabe plantearse si el Estado se convertirá en promotor de estos servicios de gran potencial educativo, facilitando el acceso a los medios electrónicos (teleconferencias, televisión por cable...) a grandes capas de población mediante su implantación en bibliotecas o en otros centros de información.

¿ES EL ESTADO EL LEGITIMO PROPIETARIO DE LA INFORMACION?

Hay un cambio sustancial respecto al punto de vista tradicional de la función del Estado en el ámbito informativo, ahora no se puede invocar el principio liberal de la abstención del Estado, porque él es el principal detentador de esa información. En este sentido, cabe recordar que la regulación de la utilización de la información por el Estado no había despertado excesiva atención hasta que aumentó la importancia de los medios de comunicación, hasta que, a causa de la evolución tecnológica y de la planificación económica, esa información se convirtió en objeto de necesidad social y propiedad económica. En concreto, la información no contingente de la que hablamos, no adquiere importancia, económica y política, hasta los años setenta, en coincidencia con la crisis económico-energética y el desarrollo de la informática.

Burkert ha planteado esta cuestión en términos de legitimidad del Estado sobre la información obtenida por éste como fruto de la recogida directa (labores estadísticas o registros públicos) o producto secundario de otras tareas administrativas [1]. Señala Burkert que la contestación a la legitimidad ha generado legislación en aspectos como la protección del secreto administrativo (que no guarda relación con una tecnología concreta) o la utilización

[1] Dice este autor que la información del sector público es exhaustiva, fiable, presentada de forma práctica y es valiosa para la elaboración de una estrategia comercial o empresarial. Desde este ámbito, el sector privado propugna que esta información ha de ser fácilmente accesible, a precio razonable o gratuita, se ha de poder elaborar sin restricciones y ha de ser distribuida con arreglo a normas de competencia justas.

de los datos personales manejados por el sector público. En ambos casos la polémica sobre los límites a las prerrogativas del Estado no está cerrada y poco a poco se abren paso esa gama de nuevas facultades consagradas en el derecho a la comunicación. Sin embargo, detrás de esta controversia sí queda claro que la información obtenida por medios legales sólo puede ser almacenada y tratada con los medios de las tecnologías de la información y que estos medios generan una información adicional cuyo valor supera a la información primaria. A su vez, esta información adicional (depuración o cruce de datos) escapa al control establecido para la recogida inicial, además de ser susceptible de un fin distinto al primario, lo que arroja nuevas sombras sobre la intervención del Estado en el ámbito informativo.

Los primeros trabajos relativos a la legislación sobre el acceso a la información del Estado datan de 1976. En ese año, la Comisión de Derechos Humanos organizó un coloquio dedicado al tema. El trabajo posterior dio lugar a una recomendación de la Asamblea Parlamentaria en 1979. Esa recomendación reconoce el derecho del ciudadano de los Estados miembros de obtener, previa solicitud, la información poseída por las autoridades públicas que no sean órganos legislativos ni autoridades judiciales. Reconoce, además los siguientes principios:

–Facilitar medios eficaces y adecuados para garantizar el acceso a la información.

–No podrá denegarse el acceso a la información alegando que el solicitante no tiene interés específico en el asunto.

–Acceso a la información con criterios de igualdad. Se exceptúan los casos de protección por razón de los intereses públicos legítimos (seguridad nacional, orden público, prevención de delincuencia...).

–Las solicitudes de información habrán de producirse en un plazo razonable.

–La denegación de acceso habrá de ser motivada, ateniéndose a las disposiciones legales y al uso.

–Podrá solicitarse la reconsideración de todas las denegaciones de información.

Estos principios no aluden a los móviles ni a los fines de los solicitantes, restringiéndose solamente en los casos mencionados, de ahí que no se excluye la utilización de esa información con fines comerciales, ni tampoco se impide la reelaboración o clasificación de la información recibida.

Para contrarrestar este derecho de acceso a la información pública que puede afectar al derecho a la intimidad de las personas, existe lo que se denomina protección de datos, cuya finalidad es restringir ese libre acceso, fundamentalmente por medios electrónicos. También ha sido el Consejo de Europa el organismo internacional que ha establecido unas pautas que buscan una solución para proteger los derechos personales, no sólo procedentes de los organismo públicos, sino que también afectan al flujo informativo entre

el sector público y el privado. En el Acuerdo para la Protección de las Personas frente al proceso automatizado de datos personales, de 1980, se establecen los siguientes principios:

–Limitación de la recogida de datos,
–calidad de datos,
–seguridad de los datos,
–especificación de la finalidad o limitación de los fines,
–Utilización restringida.
–Transparencia para las personas afectadas.
–Responsabilidad del depositario de los datos.

Para superar los obstáculos que se derivan de la aplicación de estas limitaciones, existen solo dos posibilidades: intentar obtener el consentimiento de las personas afectadas o definir previamente las condiciones de reutilización [(2)]. Así, las normas sobre protección de datos se ocupan de la protección de cada persona ante el manejo de la información automatizada, con objeto de establecer los límites de accesibilidad de los datos personales residentes en organismos públicos y el flujo informativo entre el sector público y el privado.

En síntesis, hemos visto algunos puntos de un amplio abanico de cuestiones que plantean las nuevas tecnologías en relación con el derecho del hombre a intercambiar y poner en común mensajes, contenido básico del derecho a la comunicación. Sin duda, los dos aspectos que se presentan más conflictivos son la desigualdad (cultural y económica) entre los individuos para acceder a los productos de las nuevas tecnologías y, en segundo lugar, aparece el problema capital de cómo limitar el ingente poder que concede al Estado el control de las redes y la información obtenida mediante esas tecnologías que, además de poner en peligro la libertad individual, le permite competir con ventaja en el mercado de la información.

En este sentido, la idea central que debe presidir la relación entre libertades y nuevas tecnologías es la de garantizar la libertad de emitir mensajes y la de recibirlos. Las normas que regulen esos nuevos medios deben ser conformes a la libertad de expresión, con objeto de que su ejercicio sea fácilmente asequible a todos, cualquiera que sea la configuración técnica del medio, lo que implica el derecho individual para acceder a las informaciones y a las obras que se deseen. Por su parte, el Estado debe distinguir entre su

(2) Resulta ilustrativo el ejemplo citado por Burkert sobre la legislación alemana relativa a matriculaciones de vehículos. La legislación especifica no sólo la finalidad de la recogida de información y la clase de información que puede pedirse, sino también que parte de la información puede ser transmitida a terceros del sector público y a terceros ajenos al sector público. Las factorías de coches, por ejemplo, sólo pueden obtener información personal si la persona afectada da su consentimiento en el impreso de matriculación, o bien si por motivos de seguridad se hace preciso retirar vehículos de la circulación para su revisión. Los datos útiles para la formulación de estrategias comerciales, en cambio, se les facilitan sin la identidad (H. Burkert, art. cit. pág. 7).

función constitucional de garante de las libertades individuales y la privilegiada posición de poder que las nuevas tecnologías le otorgan. Poder político y poder económico que debe estar subordinado al principio de que la última palabra la tiene el ciudadano, sin que quepa ninguna excepción para recortar su soberanía.

BIBLIOGRAFIA

BALLE, F. y EYMERY, G., Les nouveaux médias, 3ª ed., París, Press Universitaires de France, 1990.

BELL, D., El advenimiento de la sociedad postindustrial, Alianza, Madrid, 1976.

BURKERT, H., La información del sector público y el mercado de la información del sector privado. Búsqueda de una nueva legitimidad para el manejo de la información. Texto fotocopiado de una conferencia, año 1990.

FARIAS, P., voz «Derecho a la Comunicación», en Diccionario de ciencias y técnicas de la Comunicación, Ed. Paulinas, Madrid, 1991.

MERCIER, P., PLASSARD, F., y SCARDIGLI, V., La sociedad digital. Las nuevas tecnologías en el futuro cotidiano, *Ed. Ariel*, Barcelona, 1985.

PORAT, M., The information economy: definition and measurement, US Department of Commerce, 1977. RICHIERI, G., El universo telemático, G. Gili, Barcelona, 1983.

MESA N.º 7.–IMPACTO DE LA INFORMATICA EN EL DERECHO

El derecho de la informática en la formación de juristas e informáticos

MARÍA DEL CONSUELO BLÁZQUEZ ANDRÉS
Estudiante de Derecho de la Universidad de Extremadura

VALENTÍN CARRASCOSA LÓPEZ
Doctor en Derecho
Licenciado en Ciencias de la Información
Director del Centro Regional de Extremadura de la Universidad Nacional de Educación a Distancia
Secretario Judicial
Graduado Social
(ESPAÑA)

El mundo estable, tranquilizador del hombre, es hoy sólo un recuerdo. Vivimos en un mundo inquietante –maquinismo–, así nos encontramos inmersos en una sociedad que avanza a un ritmo vertiginoso; en ella se han hecho imprescindibles las nuevas tecnologías y el uso de la informática.

Si miramos a nuestro alrededor observamos que todo funciona a través del mundo informático. Y ello porque en una civilización, tal la nuestra, que viene a ser un compendio de datos, masas, números, vida competitiva, estructura y organización compleja, entre otros aspectos, la informática supone un avance en todos los campos, bien sea muy reducido o muy amplio, porque sería y es muy difícil, costoso y lento almacenar información de forma no automática. Con esto queremos decir que si la informática viene a ser el «pan

de cada día», hay que preparar y mentalizar no sólo y sobre todo a los que comienzan a abrirse camino en la lucha sino a los que ya lo hicieron y necesitan reciclarse. Sin embargo, no hablamos sólamente del aprendizaje de la informática como ciencia y como adelanto, sino también como actividad humana, en la que el individuo informático ha de percatarse de hasta dónde puede llegar y conozca que su utilización tiene un límite: los derechos fundamentales.

En la otra vertiente, que el individuo jurista analice no sólo las normas de protección de datos, entre otras cosas, sino también que conozca la práctica informática y la lleve a efecto, porque sólo así podrá catalogarla a fondo, para luchar por su buen fin y para su progreso en el quehacer diario de su ejercicio, ahorrando un tiempo y un esfuerzo, en una sociedad en la que, como decían algunos, efectivamente «el tiempo es oro».

Estamos refiriéndonos, sin duda AL DERECHO DE LA INFORMATICA. Y partiendo de esta base vamos a dividir nuestra ponencia en dos bloques:

a) El derecho de la informática en la formación de juristas, y
b) El derecho de la informática en la formación de informáticos.

A) EL DERECHO DE LA INFORMATICA EN LA FORMACION DE JURISTAS

El estudiante de derecho ha de conocer y precisa la implantación en su carrera de una asignatura: «Informática Jurídica». Y esto «salta a la vista». No es un capricho que creamos tener algunos sino una necesidad inminente y lógica.

Una vez que el alumno haya adquirido determinados conocimientos jurídicos –cuarto o quinto de carrera– se establecería dicha asignatura, para formar al estudiante de cara a su licenciatura y a su puesta en marcha en la profesión elegida. Asignatura que debe ser obligatoria, que no optativa. Y constar de dos partes. teórica y práctica, tratando de forma breve pero compendiosa aspectos tan importantes como los siguientes:

–El derecho informático.
–Protección de datos.
–Sistema registral.
–Sistema documental.
–Informática de gestión.
–Ofimática.
–Telemática.
–Informática en la Administración de Justicia.
–Correo electrónico.

Hay que señalar que estos temas son comunes y valederos tanto para el estudiante que piensa dedicarse a la abogacía, procuraduría, notaría, registro

de la propiedad, como a la administración de Justicia, como a la cátedra en derecho, etc. A todos se les habrá hecho un bien y formado como les corresponde.

Se ha dicho y con razón que algunas Facultades y, en concreto, las de Derecho viven estancadas en no sabemos qué época. Y es que ciertos sujetos y sus consejeros tienen la pretensión ilusoria de mantener su voluntad siguiendo con una enseñanza que se ha quedado anclada en el tiempo, sin tener en cuenta la realidad actual que une al jurista con la informática. Por ello, el espíritu investigador, alerta y formativo del derecho de la informática hay que empezar inculcándolo en la docencia, tanto por parte de los profesores como del alumnado. Sólo así se obtendrá un resultado coherente con el sistema que nos rodea; el licenciado en derecho no tendrá miedo a la máquina, sabrá a ciencia cierta que ésta es un arma de trabajo que utiliza y maneja a su antojo y en su ayuda, produciéndole un rendimiento máximo en pro de sus beneficios. Pretendemos que los juristas no se conviertan en «almas anquilosadas» sino en hombres del hoy y del mañana que dominan la situación porque para ello se les ha preparado. Esto es de vital importancia ya que se mueven entre conflictos humanos con una normativa, una problemática y una demanda social cada vez más extensa.

Si no se implanta en la formación de los futuros juristas el derecho de la informática –Informática Jurídica– y no se renuevan los que ya lo son, es indudable que iremos en detrimento de la verdad. Así como afirmó Miguel Angel Davara [1]...«el espíritu de iniciativa del hombre es el que ha traído como consecuencia este desarrollo tecnológico y quien viva ajeno a él, o se comporte como sujeto pasivo, siendo renuente a su utilización, comprobará como queda desplazado por el empuje de la realidad perdiendo, con el paso del tiempo, su capacidad competitiva. Algún día comprobaremos cuántos operadores jurídicos han sido rutinarios o pasivos; cuántos han perdido su capacidad competitiva, llegando al suicidio profesional».

B) EL DERECHO DE LA INFORMATICA EN LA FORMACION DE INFORMATICOS

Así como para el jurista es esencial su formación en la Informática, para el informático es igualmente indispensable su formación en el Derecho de la informática. Debiendo implantarse en su carrera –la de Informática– la Informática y el Derecho. Esto visto así, de una forma genérica, puede llamar la atención y seguro que más de uno se cuestiona la relación entre un ingeniero o un técnico con el derecho. Pues bien, se trata de una relación de considerable trascendencia, habida cuenta que estos expertos en programar no han de olvidar que no realizan sólo una labor técnica sino social. Y que

[1] Revista de actualidad Informática de Aranzadi. Miguel Angel Davara. núm. 4. julio 1992.

las normas de protección de datos, no sólo van dirigidas a los profesionales del derecho, sino a los informáticos y a los encargados de la elaboración y distribución de los programas. Y que éstos han de conocer a fondo dicha normativa, tomando verdadera conciencia de su importancia para no atropellar los derechos fundamentales de la persona. De ahí la necesidad de implantar «la Informática y el Derecho» en la formación de informáticos, como asignatura obligatoria. Se trata de infundirles desde sus comienzos un sistema moral que regule sus actividades futuras, para que ante todo y sobre todo mantengan una ética profesional acorde con uno de los bienes más preciados del hombre: el derecho a la intimidad.

Que se percaten que no son sólo técnicos-informáticos, ingenieros, programadores o como quiera llamárseles, sino que realizan o realizarán una tarea mucho más profunda que atañe a la generalidad y, por tanto, deberán delimitar el ejercicio de su profesión con arreglo a la Ley y a los derechos humanos. Y para ello, nada mejor que formar a los estudiantes de informática en esta línea. No cabe duda que sería una mezcla perfecta: técnica y humanismo.

Creemos firmemente en la necesidad de El Derecho de la Informática en la formación de juristas e informáticos, porque hay razones de peso, tales como las expuestas en esta ponencia, que así lo verifican. Los Organismos y Autoridades competentes no pueden cerrar los ojos ante tan evidente realidad, debiendo renovar la metodología de la enseñanza creando un nuevo plan de estudios con personal cualificado impartidor de lo que se ha venido a denominar «Informática Jurídica» e «Informática y Derecho», en pro de esta generación y de las generaciones venideras. Estamos ante una exigencia inaplazable que no puede dar lugar a demora de clase alguna. Que el futuro informático o jurista no se siente en un aula y se pregunte ¿Qué pasó, acaso nos hemos anclado aquí como un buque naufragado al fondo del océano?

El Working-House informático o tele-trabajo

EDUARDO DE NO-LOUIS Y CABALLERO
Licenciado en Derecho.
Master en la C.E.O.E. de Relaciones Laborales
(ESPAÑA)

I. INTRODUCCION

Desde el momento en que el hombre lanzó el primer sonido y aprendió que con él podía transmitir ideas y sentimientos haciéndose entender por los de su especie, hasta las avanzadas técnicas de comunicación que hoy día utilizamos tan sólo ha variado el medio en que recogemos el mensaje que queremos transmitir.

I.1. HISTORIA DE LA COMUNICACION HUMANA

Primeramente fue, como se ha visto, la comunicación denominada boca-oído, en la que el mensaje partía del sujeto fuente mediante sonidos guturales, al receptor que lo interpretaba. Posteriormente los sonidos se plasmaron en signos escritos y así el mensaje pasó de las ondas sonoras a quedar impreso, facilitando su conservación en el tiempo.

Fue a mediados del Siglo XIX, en 1844, cuando el Norteamericano SAMUEL FINLEY B. MORSE, inventó la comunicación mediante impulsos electromagnéticos a través del Telégrafo (transmisión de signos), fortaleciéndose con él la noción de telecomunicación como procedimiento de transmisión de información mediante señales ópticas, acústicas, eléctricas o electromagnéticas a distancias superiores a las normalmente alcanzadas por la voz humana.

Pocos años más tarde, en 1876, el Británico ALEXANDER GRAHAM BELL inventó un aparato capaz de convertir la voz humana u ondas sonoras en

variaciones de corriente eléctrica, susceptibles de ser enviadas mediante un cable eléctrico (línea telefónica) a otro aparato receptor que a su vez las modula en ondas sonoras, el teléfono o transmisión de sonidos.

Ya tan sólo nos queda un paso, que aún no se ha terminado de dar, que es la transmisión interactiva tanto de la voz como de la imagen y que es hoy posible gracias a la avanzada tecnología informática, digital y de los satélites que proporcionan la simultaneidad de la videocomunicación como transmisión de imagen y sonido desde un punto central de emisión hasta los abonados, y en algunos casos permite señales de retorno desde los extremos hacia la cabecera de la red o punto central de emisión. Dos aplicaciones de este concepto son:

LA VIDEOCONFERENCIA: servicio que permite la comunicación bidireccional simultánea, persona a persona o grupo a grupo, para el intercambio de diversos tipos de información tanto de audio como de video, con imagen en movimiento o fija, gráficos textos, datos, de forma interactiva y en tiempo real que proporciona la capacidad de telereunión de usuarios geográficamente dispersos y distantes.

LA VIDEOTELEFONIA: servicio audiovisual simétrico y bidireccional, en tiempo real, para el intercambio persona a persona de voz e imágenes tanto en movimiento como fijas, excepcionalmente puede admitir también la transmisión de datos textos y gráficos[1].

I.2. DE LA COMUNICACION ORAL A LA TELEMATICA

Junto a estas formas de comunicación o telecomunicación bidireccionales o interactivas, es decir, que posibilitan la emisión de otro mensaje de respuesta por parte del sujeto receptor, creando una intercomunicación entre ambos.

Existen otros medios de comunicación unidireccionales en los cuales el mensaje sólo fluye en un sentido, del emisor hacia el receptor, sin posibilidad de retroalimentación o respuesta por parte del sujeto que la recibe, como por ejemplo son la televisión como transmisión a distancia de imágenes en movimiento o la radio.

Sin embargo, poco a poco la televisión está transformándose en terminales a domicilio, a través de los cuales el usuario puede interrogar determinados bancos de datos. Ha dejado o están dejando de ser meros receptores de imágenes para ser procesadores de secuencias (TELEORDENADORES) que almacenarán, manipularán, crearán y transmitirán información o programación digital, lo que creará conflictos respecto al dominio de los Protocolos de Unión o de Interconexión entre los diversos equipos, como señala el IN-

[1] * N.A.:Experiencia que ha realizado con éxito la empresa SINTEL los días 6 de mayo a 3 de junio en las oficinas de la c/ Pedro de Valdivia, y el día 27 de junio de 1992 en la CAMARA DE COMERCIO de MADRID, para las cuales está creando una red de salas de videoconferencias.

FORME NORA-MINC encargado por el Presidente de la República Francesa, y al que luego me referiré.

La mayoría de las personas que reciben información pasivamente, como si les viniera de lo alto, a través de terminales no inteligentes, acertadamente denominadas «cajas tontas», podrán con el teleordenador intercambiar, manipular y visualizar diversidad de información interactuando directamente, lo que ampliará la posibilidades de comunicación. Por último la Teleinformática o telemática como conjunto de técnicas, que permiten la comunicación entre varios equipos informáticos, de ordenador a ordenador, a través de una red de telecomunicación que constituye su espina dorsal pues está compuesta por las redes de transmisión de datos tanto a nivel local, nacional o internacional, por las que circularán informaciones informatizadas, es decir, sometidas a tratamiento informático que comprimen el mensaje y lo convierten en impulsos eléctricos capaces de ser transmitidos a muy alta velocidad por la red de telecomunicación.

II. DEFINICION DEL WORKING-HOUSE INFORMATICO O TELETRABAJO

Dentro de las posibilidades que ofrece la teleinformática o telemática está el denominado teletratamiento como ejecución de una acción o de un proceso a distancia que implique el uso de un equipo informático y de una red de telecomunicación, en la que se establezca una bidireccionalidad de la información en tiempo real. Como características podemos señalar la conexión de dos o más equipos informáticos, que están distantes entre sí, que implique la ejecución de una acción o un proceso y que éste sea de forma bidireccional, es decir que exista entre ellos una intercomunicación en tiempo real realizada a través de una red de transmisión de datos con un lenguaje protocolarizado o inteligible para los equipos implicados. En este proceso una parte de la información bidireccional va dirigida a la adopción de las medidas de control que aseguren la fiabilidad de la comunicación, tanto para la propia comunicación del mensaje como para el contenido del mismo. Los sensores de control captan las incidencias del estado o proceso de comunicación y los transmiten al centro de dirección para que ordene las acciones de control pertinentes a adoptar.

Dentro del concepto de teletratamiento han surgido diversas modalidades que podemos agrupar en dos grandes áreas A) LA TELEACCION: que permite la actuación o supervisión de un conjunto de elementos en tiempo real controlados o supervisados a través de redes de telecomunicación y que comprenden acciones tales como el telecontrol, la telemedida, la telealarma o la teleseñalización; y otra B) EL TELETRABAJO: concepto que nació recientemente en Europa a mediados de los años setenta para una serie de Empresas que se vincularon a las nuevas tecnologías de la información para la realización de sus actividades.

La noción de teletrabajo ha ido tomando un carácter muy amplio, lo que dificulta una definición concisa del término, pero que podemos conceptuarlo como «todas aquellas actividades profesionales desarrolladas a través de un equipo informático, que hacen uso de las técnicas de teletratamiento y telecomunicación para enviar información en tiempo real al centro de trabajo, producción o servicios y que genera un valor añadido a sus usuarios».

Estos servicios de teletratamiento aportan nuevas facilidades gracias al uso combinado de sistemas informáticos y redes de telecomunicación, que abren nuevos campos de aplicación, potenciando actividades empresariales tales como la disponibilidad de servicios remotos, el acceso al teletrabajo la automatización de funciones a distancia (tan empleadas hoy en los llamados edificios inteligentes u hogarótica), o la descentralización de empresas. Todo ello conlleva a la ampliación de posibilidades de explotación de los sistemas de telecomunicación, que corren el riesgo de quedarse rápidamente obsoletos, si no evolucionan adecuadamente, frenando con ello la expansión de la telemática y del teletratamiento. Ya que si consideramos, por ejemplo, que los alambres de cobre convencionales que operan a cuatro kilohercios, pueden manejar un total de 9.600 Bits/sg. algo más si se comprimen por un modem de alta velocidad, cantidad claramente insuficiente para los 200 millones de Bits/sg. que son necesarios para la combinación de imágenes de alta definición en movimiento con sonido de alta fidelidad, hoy tan sólo alcanzables por medio de la fibra óptica.

Es precisamente este uso combinado de sistemas informáticos y de redes de comunicación el que ha propiciado el nacimiento del WORKING-HOUSE INFORMATICO O TELETRABAJO, como un trabajo realizado a través de un equipo informático, fuera del centro de trabajo (conceptuado como Empresa) y enviado a él mediante una red de telecomunicación.

Si desglosamos la acepción propia del término como «tele» distancia y «trabajo», es decir, trabajo a distancia que los Norteamericanos han denominado, reduciendo el término como trabajo en casa «Working-House» (que es una de las modalidades del teletrabajo). Tal confusión o denominación errónea quizás sea debida a la similitud fonética con la palabra «working hours» que significa jornada de trabajo.

II.1. CLASES O TIPOS DE WORKING-HOUSE

Como primera modalidad, analizaré la ya comentada del trabajo en casa, en ella la unidad de trabajo o equipo informático se encuentra en el domicilio del trabajador que es donde se procesa la información para posteriormente ser enviada a la Empresa o al cliente.

En 1.986 se estimaba que un millón de personas trabajaba con terminales en sus hogares y que este número se habrá cuadruplicado para 1.995, sin embargo, a un 61% de los encuestados no le agradaría sucumbir al cómodo

enclaustramiento del teletrabajo doméstico, tan ventajoso para amas de casa, ancianos o impedidos físicos.

El trabajo móvil, como un subgrupo, en el cual se utiliza para la telecomunicación entre la Empresa y el personal que se encuentra desplazado del centro de trabajo.

La oficina descentralizada, para aquellas Empresas que cuentan con departamentos distribuidos en diferentes lugares.

El PIECEWORK informático como trabajo a destajo o tarea que es enviada al ordenador central de la Empresa o centro de trabajo telemáticamente, igual ocurre con el TIME-WORK informático, como trabajo realizado a tiempo y que es enviado a la unidad central por un proceso de telecomunicación. En ambos casos es el ordenador central el que va acumulando la totalidad de la información en que se ha desglosado el trabajo, suele utilizarse para evitar en lo posible la denominada piratería informática como captación de datos por receptores a los que no les iba dirigida la información.

Por último el CUSTOM WORK o trabajo realizado a medida, es un teletrabajo encaminado a la creación de un software específico que es enviado a otro equipo informático, por un medio de telecomunicación, en el cual se va a aplicar.

II.2. IMPLICACIONES

El teletrabajo viene a permitir la volatilización de la oficina colectiva, que será sustituida por multiplicidad de centros o lugares descentralizados, de decisión o control y por su deslocalización, separación geográfica de los centros de trabajo, lo que implicará quizás una nueva revolución industrial menos traumática que la del siglo XIX, e implantada esta vez en el sector terciario o de los servicios.

II.2.1. CREACION DE UNA RED ADECUADA DE COMUNICACIONES

El sector de las telecomunicaciones, que siempre ha estado en contacto con la informática, está integrándose cada vez más con ella, los canales para transmitir información se están interconectando creándose modos específicos para la comunicación entre ordenadores que a su vez están controlados por otros equipos informáticos, como señala el profesor MARIO G. LOSANO.

Pero de esta interconexión, surge un problema, tal y como apunta el Informe NORA-MINK en los siguientes términos «Mientras que hasta ahora los conflictos se referían a las máquinas, de ahora en adelante se referirán al dominio de los Protocolos de Unión, por tanto una nueva división del poder tendrá lugar entre constructores de redes de comunicación y gestores de satélites, a éstos les corresponderá definir las nuevas reglas del juego».

Uno de los Protocolos que regulan el Teletrabajo es el denominado E.D.I.(*) que se define como la transmisión electrónica de información, de ordenador a ordenador, de tal modo que pueda ser procesada automáticamente sin intervención manual.(*– Electronich Data Interchange.)

Es fundamental que esta red de transmisión se ocupe de recoger la información del sistema emisor y entregarla en los destinos apropiados sin error, formando parte de esta red estarán: por un lado los medios de transmisión y por otro los sistemas de tránsito que permiten la transmisión de datos de forma adecuada, compuestos por cables coaxiales, fibras ópticas aparatos de amplificación de señal, etc...

Esta red enlazará mundialmente hogares y oficinas uniendo equipos informáticos entre sí, su composición será seguramente la fibra óptica interactiva que con sus 100 Megabits/sg velocidad a la que está normalizada se expandirá como una gran tela de araña atravesando el Planeta para invadir nuestro hogar como antaño lo hiciera la luz eléctrica, como suministro de energía, o la red telefónica, como suministro semántico. Ahora tendremos un suministro de impulsos lumínicos positivos y negativos que se convertirán en imprescindibles. DICHTER no pudo imaginar quizá, en su bella metáfora acerca del hogar, concebido como «una caverna aterciopelada», lo acertado que era su pensamiento.

El teleordenador necesita de una red digitalmente conmutada que ofrezca un amplio espectro y gran densidad de comunicación, tal posibilidad viene proporcionada hoy por la fibra óptica, que utilizando ondas de luz visible e infrarroja supone un claro avance sobre el ya saturado espectro electromagnético. Pero la fibra óptica es simplemente uno de los muchos modos de agrandar la disponibilidad del espectro electromagnético y quizás puerta de entrada al «telecosmos», en donde la longitud de onda es millones de veces más corta que las hoy empleadas, y que se realizan a la velocidad de la luz, es la llamada optoelectrónica que combinará la tecnología electrónica con la tecnología fotónica.

Por ejemplo utilizando esta fibra de vidrio y luz será posible transmitir toda la colección de la Biblioteca del Congreso de los E.E.U.U. en ocho horas, lo que hoy requeriría poco más o menos de unos doscientos años por líneas convencionales de cobre.

II.2.2. REPERCUSIONES EN EL SER HUMANO A NIVEL SOCIOLOGICO Y PSICOLOGICO

El Japón está decidido a llevar la fibra óptica a la mayoría de sus hogares y oficinas a comienzos del próximo siglo, lo que puede producir que los costes de las Empresas Japonesas estén, de conseguirlo, muy por debajo de los costes de Empresas Norteamericanas, no siendo entonces éstas competitivas necesitando por tanto de una reconversión, con los subsiguientes desajustes sociales, dependiendo quizás la hegemonía mundial de ello, ya que en el

espectro electromagnético terrestre, en donde todo empieza a moverse a la velocidad de la luz no existirán refugios nacionales en donde poder guarecerse de la competencia.

El Teletrabajo, a través de la Telemática o el Teleproceso, con sus veloces flujos de información, solucionará multitud de problemas, podremos contratar cualquier servicio desde nuestro propio hogar, podremos trabajar desde nuestra habitación e incluso nuestra vivienda estará regida por microprocesadores programables capaces de controlar las más elementales tareas domésticas que podrán ser activadas, incluso por control remoto. Podrá contribuir a mejorar el tráfico urbano incidiendo en la solución de la contaminación y los atascos, creando una pantallización de la Sociedad, un enclaustramiento del individuo que fácilmente sucumbirá a las seductoras comodidades de la técnica hipotecando parte de su movilidad y libertad condenándose a un larocentrismo narcisista socialmente patológico.

Conllevará además un elevado grado de sedentarismo una grave mutilación de las experiencias sensoriales y en definitiva un aislamiento psicológico y social, será pues el triunfo de la Sociedad hermética y claustrofílica en la que los individuos agorafóbicos, sentirán un estado de angustia y vértigo cuando se vean solos ante espacios abiertos amplios y libres, en contraposición a la Sociedad agorafílica en la que vivimos (lo que NORA y MINK llamaron con triunfalismo el «agora informacional»).

Será una nueva Sociedad informatizada, segmentada en células hogareñas autosuficientes e interconectadas por medio de una escritura fosforescente, compensando el aislamiento de los individuos con una nueva cultura de la sensorialidad, de la tactilidad y del diseño, de la creación de imágenes fascinantes e innovadoras.

III. INCIDENCIA DEL WORKING-HOUSE EN EL MUNDO DEL DERECHO

Todas estas innovaciones técnicas tanto en el mundo de las telecomunicaciones como en el mundo de la informática tendrán que venir respaldadas por el Derecho como canalizador y regulador de realidades sociales, como protector de la esfera de individualidad e intimidad de las personas y de sus intereses. Posibilitando el uso pacífico y normado de la tecnología para el resto del colectivo humano.

III.1. A NIVEL INTERNACIONAL

No cabe duda que serán necesarios una multitud de Tratados Internacionales en los cuales se regulen de forma específica la transmisión de datos telemáticos entre Estados. Quién sabe si pudiera crearse un Organismo Internacional «integrado como una modificación a la Carta de San Francisco» que

se ocupará tanto de canalizar los nuevos procedimientos como de dictar y aplicar la Normativa Internacional referente a estas materias.

Por otro lado, se tendrá que llegar a acuerdos de normalización, protocolos, que permitan el intercambio de datos informáticos telemáticamente. Aunque para ello es necesario llegar primero a un lenguaje común para toda la Humanidad, destructor de la Torre de Babel, que quizás esté compuesto por una luz intermitente, centelleando impulsos positivos y negativos a velocidades impensables o por el estridente chirriar de un equipo informático.

Hoy las distintas legislaciones nacionales e incluso algunas internacionales se han dedicado a la protección de los denominados bancos de datos, que como en las antiguas bibliotecas monacales, es donde se está concentrando el conocimiento humano, dejando desprotegidas las vías por donde circulan las informaciones (redes de telecomunicación).

Sin embargo cada vez es más seguro y firme el paso de los distintos ordenamientos jurídicos tanto nacionales como internacionales, en la creación de las normativas específicas que regulan, protegen y limitan el uso de la informática dentro de la mayor acepción del término.

Vemos así entre ellas, las del Departamento de Defensa Norteamericano, recopiladas en el llamado Libro Naranja, la Normativa POSIX DEL I.E.E.E. (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS), La Ley de Protección de Datos Personales de Austria, La Ley de Acceso a la Información y Protección de Datos de Canadá, La Carta del Usuario de Programas de la C.E.C.U.A.(Confederación de Asociaciones Europeas de Usuarios de Ordenador), Las Directivas de la C.E.E. 77/62, 80/767, 86/361, 87/95, 88/295, y 85/374. Sin embargo la entrada en el Mercado Unico el 1 de Enero de 1.993, supondrá una serie de cambios o modificaciones en las normativas de las diferentes áreas de los Ordenamientos Jurídicos de los distintos países que integran la Europa Comunitaria. Bruselas está trabajando en la elaboración de una serie de Directrices que armonicen y unifiquen criterios de las legislaciones nacionales de sus Estados miembros sobre tres campos:

A) Sobre la protección legal de software que ya cuenta con acuerdos adoptados y que al parecer afectará directamente a nuestra L.P.I. (Ley de Propiedad Intelectual), cuyo texto tendrá que ser modificado o adaptado en parte.

B) Se centra en la redacción de un texto que unifique y delimite la protección de los datos e intimidad de la información teniendo también como objetivo la armonización de la legislación en lo concerniente a redes de telecomunicación.

C) Por último el tercer campo se centrará en la responsabilidad por servicios defectuosos.

El Convenio 108 del Consejo de Europa o el Tratado Internacional para la Protección Legal de Programas, Propiedad Intelectual y Transferencia de

Tecnologías (recomendaciones WIPO, World Intellectual Propiety Organization), entre otras, por destacar algunas de la gran multitud de Normas que con carácter Internacional o Nacional inciden en la regulación de los procesos informáticos.

III.2. REPERCUSIONES EN EL ORDENAMIENTO JURIDICO ESPAÑOL

Nuestro Ordenamiento Jurídico no es indiferente a los cambios operados en el mundo de la informática, ya desde el año 1.978 en que surgieron la primeras normas sobre Derecho Informático, hasta la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal) que en su art. 32 y ss., se ocupa del movimiento internacional de datos. Así mismo hay que citar dos normativas básicas a tener en cuenta. Por un lado lo previsto en la Ley Orgánica de las Telecomunicaciones teniendo en cuenta lo dispuesto en el denominado Libro Verde de las Telecomunicaciones y por otro la Ley de Propiedad Intelectual, de 17 de Nov. de 1.987 que le dedica su título VII «De los programas de ordenador», preceptuando que «se entenderá por programa de ordenador, toda secuencia de instrucciones destinadas a ser utilizadas directa o indirectamente en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado cualquiera que fuese su forma de expresión o fijación».

Por tanto el producto del teletrabajo no puede ser considerado propiamente como un programa informático, pero sin embargo debería gozar de la misma protección legal de éstos, pues considero que tal es el espíritu de la ley cuando establece los siguientes términos «...toda secuencia de instrucciones destinadas a ser utilizadas, directa o indirectamente» el teletrabajo sería pues una utilización indirecta de un equipo informático.

En cuanto a la protección de los datos informáticos en el momento de la telecomunicación, nuestro Ordenamiento Jurídico sigue la tónica general, dedicándose a una regulación de los datos en el momento en que los mismos permanecen estáticos en la base de datos y no cuando circulan telemáticamente por la red de telecomunicación. Así el título V de la LORTAD arts.32 y 33 prohíbe «la transferencia de datos de carácter personal objeto de tratamiento automatizado con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley».

En iguales términos se pronuncia la Ley 10/91 de la República Portuguesa, «al restringir la interconexión de ficheros automatizados para los datos personales de carácter policial criminal o médico» (Cap.V, arts. 22 a 26). Quedando a sensu contrario, permitida la transmisión de datos que no se incluyan dentro del concepto de datos personales de carácter sensible «datos sensibles», es decir, aquellos que inciden directamente dentro de la órbita de la individualidad y libertad de la persona humana.

III.2.1. DERECHO LABORAL

Si bien no existe hoy por hoy una normativa específica directamente aplicable al teletrabajo, el Estatuto de los Trabajadores es lo suficientemente amplio para acoger la figura, ya que si se cumplen los condicionamientos recogidos en su art. 1 para aquellas personas que presten sus servicios voluntariamente por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, mediando una remuneración, se dará una relación laboral, con lo cual serán de aplicación todas las normativas vigentes del Derecho Laboral e incluso aquellas que por Convenio Colectivo o pacto individual pudieran establecerse específicamente.

En lo referente a las relaciones con la Seguridad Social, viene posibilitando la Dirección General de la Tesorería de la misma, que la información que obligatoriamente se le ha de facilitar le sea presentada en soportes magnéticos cuando expresamente así lo autorice; vislumbrándose la posibilidad de que dicho tráfico se termine realizando telemáticamente mediante el teletrabajo, en un futuro no muy lejano, proporcionando mayor eficacia y celeridad en el desarrollo de sus cometidos.

III.2.2. DERECHO PENAL

El uso de la informática, que tantas posibilidades ofrece al mundo de los humanos, convirtiéndose en un elemento cada vez más indispensable, empieza a presentar graves inconvenientes, unas veces, debido al propio uso de los equipos informáticos, otras, por ser objeto de ataque o el medio para cometer delitos, lo que hoy se conoce como «Criminalidad Informática» ya que dadas sus especiales características la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas que pueden encuadrarse en dos grandes áreas: A) aquellas que persiguen o denotan un carácter patrimonial, tales como estafas, alzamientos, apropiaciones indebidas... y B) aquellas que inciden en el tratamiento manipulación, sustracción de datos o informaciones de bases de datos que darán lugar a delitos tales como falsedades, descubrimientos y revelación de secretos, ataques a la intimidad personal etc...

Alguna de estas conductas, por su singularidad han llegado a alcanzar denominación propia.

Tal es el caso de DATA DIDDIING, o introducción de datos falsos que manipulen transacciones de entrada en el equipo informático produciendo movimientos falsos de información, EL TROJAN HORSE, virus informático que a base de introducir instrucciones erróneas en los programas de uso habitual lleva al ordenador a que actúe de forma anómala, EL ROUNDING DOWN o técnica del salami, que se emplea para encauzar o sisar pequeñas cantidades de unas cuentas para pasarlas a otras ficticias, EL SUPERZAPPING, es el uso ilícito de un programa de ordenador para alterar, borrar,

copiar, insertar, o utilizar datos almacenados en un equipo informático o en una base de datos, EL TRAPS DOORS, o puerta falsa, son entradas o accesos a programas utilizados temporalmente para chequeos, y que al no ser borrados permiten el acceso al programa de otros usuarios no autorizados, LOGIC BOMBS, o bombas lógicas, son instrucciones que se autoactivan, mezclando o borrando la información o inutilizando el equipo informático, quizás el ejemplo más conocido es el denominado virus VIERNES 13, se suelen activar un día determinado o pasado un lapso de tiempo o por número de encendidos del equipo informático; SCAVENGING recogida de información residual que ha quedado residente en la memoria del ordenador o en los soportes magnéticos mediante su restauración; EL WIRETAPPING, pinchado de líneas de telecomunicación para introducirse en ellas y recoger, manipular, borrar información de bancos de datos o introducir información falsa, tal conducta la realizan los denominados HACKERS. Por último recoger aquí todas aquellas conductas que conllevan la sustracción tanto de dinero, como de mercancias, servicios, software, o información.

Nuestro Ordenamiento Jurídico Penal vigente no ha contemplado ninguna de las conductas anteriormente descritas y es por medio de la interpretación jurisprudencial como se van resolviendo muchas de dichas cuestiones; que al final se ven encaminadas hacia un simple delito de daños. Sin embargo, el Anteproyecto de Nuevo Código Penal, recoge acertadamente, como tipos delictivos algunas de ellas, así en su título IX «Delitos contra la Intimidad y el Domicilio» se ocupa en el Cap. I de los «Delitos contra la Intimidad y el Secreto de las Comunicaciones» arts. 194 a 196, o en el Cap. VI, Secc. I art. 248 apdo. 2 que preceptúa: «...cometen estafa ... los que realizaren una manipulación informática que interfiera el resultado de un procesamiento o transmisión informática de datos y... ocasionen perjuicios a otros». Además la Secc. III del Cap. VI protege la infracción de los Derechos de Propiedad Intelectual castigando a quienes «... reprodujeren, plagiaren, distribuyeren o comunicaren... en todo o en parte... una obra literaria, artística o científica ... fijada en cualquier tipo de soporte o comunicada a través de cualquier medio.»

Artículos, que entre otros, convierten al Anteproyecto de Código Penal, en algo innovador en materia de Derecho Informático, tanto a nivel nacional como internacional, adecuando y acercando el Derecho a la realidad social.

III.2.3. DERECHO MERCANTIL

Quizás sea el Derecho Mercantil quien más ha innovado en esta materia, al recoger dentro de la Ley de Propiedad Intelectual un título dedicado a los programas de ordenador (arts. 95 a 100) en donde se hace un detallado análisis de los aspectos más relevantes en cuanto a los derechos de autor, de explotación o cesión, sin embargo dicha legislación tendrá que amoldarse

próximamente a las Directivas Comunitarias que sobre la materia se dicten con el fin de armonizar las diferentes legislaciones nacionales.

Otra innovación en el Derecho Mercantil es la de poder interactuar telemáticamente dentro del mercado de valores para la contratación y control de títulos cotizables en Bolsa.

IV. CONCLUSION

El camino hacia el futuro está en la integración de los sistemas, tal interconexión permitirá ahorrar energía y aumentar el confort, hombres, técnica y naturaleza podrán convivir en una relación vital, constructiva y productiva, gracias a lo que se está empezando a denominar NETWORKS o Sistemas Interconectados, de los cuales el TELETRABAJO es o constituye un pequeño paso que se está comenzando a dar, dando vida a la metáfora: «No podemos predecir el futuro, pero lo podemos inventar».

Derecho consuetudinario indígena y la informática

CARLOS DURAND ALCÁNTARA

Profesor Investigador del Area de Ciencias Sociales –Derecho Agrario– de la Universidad Autónoma Chapingo. Doctorado en el Instituto de Investigaciones Antropológicas de la Universidad Nacional Autónoma de México. Profesor de la Escuela Nacional de Estudios Profesionales «Zaragoza» de la UNAN.

DANIEL RIVERA SALGADO

Profesor Investigador del Area de Ciencias Sociales de la Universidad Autónoma Chapingo. Profesor Investigador de Agroecología de la U.A.CH. Maestro en Ciencias (Especialidad Geografía). Profesor Investigador del Area de Humanidades de la Universidad Autónoma Metropolitana.

(MEXICO)

1. PLANTEAMIENTO DEL PROBLEMA

La Nación mexicana es pluriétnica y multicultural, circunstancia que se deriva del mosaico de poblaciones indias existentes en su territorio.

El pasado y el presente de la formación social mexicana se encuentra impregnado de múltiples contribuciones que en todos los órdenes de la vida económica y social han desarrollado estos pueblos. Qué decir de las aporta-

ciones que en materia de ciencias factuales nos brindaron culturas como la maya y la azteca; la tecnología mixteca y tolteca, el arte purépecha y en la actualidad, las aportaciones de las 56 etnias del país en materia de medicina tradicional, aspecto que incluso, viene reproduciendo el conjunto de laboratorios de la industria químico farmacéutica a nivel internacional.

Aunque aún subsisten concepciones racistas, es importante reconocer que los pueblos indios representan una de las raíces más significativas para recuperar nuestras propias identidades y que su presencia enriquece la diversidad socio-cultural de México.

Atendiendo al criterio lingüístico y a su cuantificación censal, se sabe que el 15.8% de los mexicanos habla solo lengua india[1].

Esta población se agrupa en 56 etnias de diferente magnitud, teniendo cada una su propio idioma y se distribuyen a lo largo de todo el territorio del país.

En los Estados de Oaxaca, Quintana Roo y Yucatán, la población indígena representa más de la mitad del total; en Campeche, Chiapas e Hidalgo es superior a la cuarta parte; en Guerrero, Puebla, San Luis Potosí y Veracruz es superior al 10%. En los demás Estados, la población indígena queda por debajo del 10% del total, aunque es mayoritaria en determinadas regiones. La etnias más numerosas se encuentran presentes en más de una entidad federativa, entre ellas destacan los pueblos nahuatls, maya peninsular, nañhu y mixteco. Cuando menos un millón de indios habitan en el área metropolitana de la Ciudad de México[2].

En la actualidad se calcula que en el país habitan alrededor de diez millones de indígenas[3].

No obstante la importancia y significado de estos pueblos, el Estado mexicano no ha reconocido en su justa dimensión sus derechos.

1.1 La legislación mexicana y los pueblos indios.

El sistema jurídico en que se ubican las etnias es atípico en su realidad.

El régimen legal contiene insuficiencias graves al integrar a individuos poblaciones distintos del conjunto nacional, a la sociedad mexicana. De esta forma el régimen normativo ha resultado insuficiente e incongruente con la racionalidad en que se desenvuelven los indios.

La Constitución mexicana contiene un enfoque positivista acorde con el paradigma capitalista que le dió vigencia. De esta manera el bloque dominante negó la condición de diversidad de las poblaciones indias[4] y su posible

---

[1] (INEGI: 1990).

[2] (INEGI: 1980).

[3] (Valdéz: 1988).

[4] Una de las mayores dificultades a las que se enfrentan los autores de estos y otros estudios, es definir «las poblaciones indígenas».

En efecto, a través de la lectura de los diferentes instrumentos internacionales, se advierte

desarrollo autónomo. El Edo., mexicano aplicó en su legislación un criterio monoétnico ... el del bloque hegemónico, hecho no gratuito sino producto del discurso de poder de dicho bloque, cuyo proyecto plantea la homogeneización sociopolítica y la omisión jurídica de las poblaciones indias, como un hecho necesario y útil para la reproducción y expansión de su sistema.

La expresión jurídica de esta hegemonía se encuentra, entre otros, en los preceptos contenidos en el art. 30 de la Constitución General de la República[5] en los que se establece que toda la población existente en el territorio nacional adquirió su estatus de ser «mexicana».

Otro aspecto que asienta la Constitución es el de la igualdad ante la ley. Conforme a éste formulismo jurídico todos los mexicanos son «iguales» frente al derecho, aspecto que se fundamenta en el Título I, Capítulo I referente a las garantías individuales. Teórica y doctrinariamente este tipo de principios es irrefutable; sin embargo, en los hechos este pronunciamiento «homogeneizó» a 56 etnias para corporativizarlas al proyecto nacional, con lo que se hizo «iguales a los desiguales».

En diciembre de 1990 el ejecutivo federal decretó el «reconocimiento de los pueblos indios», al ser adicionado el art. 4 constitucional[6], aspecto que fue multicriticado por los especialistas e investigadores de «la cuestión étnica» aludiendo a su esencia culturalista, desvirtuadora de los intereses indios, además de haber considerado los problemas de índole socioeconómico y político en que se encontraban las etnias del país.

Este fue el marco jurídico en el que el gobierno promulgó el 6 de enero de 1992 reformas y adiciones al art. 27 Constitucional, las que advertimos, relativizarán, aún más, los derechos sociales y humanos de los pueblos indios.

---

que no existe una definición que englobe a todas las poblaciones que pudieran responder a este concepto. Cada país ha planteado el problema de la definición a su manera, habiéndose llegado así a nociones que abarcan una amplia gama de criterios de diferenciación, desde factores exclusivamente raciales, hasta consideraciones en que predominan criterios socio-culturales. No solamente existen definiciones distintas y a veces contradictorias, sino que también denominaciones distintas; así encontramos entre otras: «poblaciones indígenas», «aborígenes», «nativos», «silvícolas», «minorías lingüísticas», «indios», o simplemente «tribus», «tribus semibárbaras», «poblaciones no civilizadas», «poblaciones no integradas», «autóctonos», «poblaciones autóctonas», y a este propósito debemos agregar que a veces en un mismo país se utilizan definiciones y criterios distintos para definir o catalogar porciones de la población del estado o nación, lo que hace el problema más complejo. (Stavenhagen: 1988).

Erica Daes menciona que en la mayoría de países aceptan el término poblaciones indígenas, a diferencia del de pueblos, naciones, comunidades, etc. Erica Daes fue presidenta de la subcomisión para la prevención de las discriminaciones y la protección de las minorías. (Daes: 1988).

[5] Constitución política: 1992.

[6] Decreto que adiciona un primer párrafo al art. 4 de la Constitución Política, recorriéndose en su orden los actuales párrafos primero a quinto, para pasar a ser segundo a sexto respectivamente, en los siguientes términos: Art. 4 La Nación mexicana tiene una composición pluricultural sustentada originalmente en sus pueblos indígenas. La ley protegerá y promoverá el desarrollo de sus lenguas culturas, usos, costumbres, recursos y formas específicas de organización social y garantizará a sus integrantes el efectivo acceso a la jurisdicción del Estado. En los

En particular el artículo 27 Constitucional define, entre otros aspectos, las relaciones de propiedad que subyacen en el campo mexicano, representando ello un aspecto medular para las etnias del país, ya que, en gran medida su sobrevivencia dependerá del control que ejerzan sobre sus territorios y del dominio que establezcan sobre sus recursos.

1.2 Marco socioeconómico rural y reformas al art. 27 Constitucional.

La proyección de los precipitados cambios, tanto a nivel urbano, como rural se ubican en el contexto de la globalización y postmodernización que vienen impulsando los grandes oligopolios a nivel mundial y cuya tendencia específica es la del ensanchamiento del capital productivo en el agro, con sus respectivas escuelas de expulsión de amplios sectores de campesinos minifundistas (indios), sin que necesariamente se garantice su posible empleo y la intensificación de su pobreza. Al respecto Antonio García mencionaba: «La modernización propiamente capitalista concentra entre el 40 y el 65% de la mejor tierra de labor y sólo emplea entre el 4 y el 6% de la fuerza de trabajo agrícola... Esta enorme concentración de la propiedad territorial contrasta dramáticamente con la excesiva parcelación de las regiones de minifundio en donde no más del 3 al 5% de la tierra agrícola se aglomera entre el 50 y el 70% de la fuerza de trabajo rural[7].

Socialmente estas políticas modernizadoras amenazan seriamente la supervivencia de los pueblos indios[8], al respecto encontramos que según datos elaborados por la C.E.P.A.L.[9], se calculaba que para 1989 el número de pobres en América Latina había aumentado a 183 millones, estableciéndose un nuevo adjetivo, el de pobreza extrema, concepto que se adecuó a las poblaciones indias y a las áreas marginadas suburbanas del continente.

En particular en México, esta pobreza extrema ha derivado en la muerte por inanición, alcanzando un rango de cien mil niños[10], además de que en el medio rural la crisis agrícola se ha profundizado, con sus respectivas manifestaciones de polarización social. Al respecto Calva refiere: «El campo mexicano resiente el flagelo de una nueva crisis agrícola, la cosecha de granos para consumo humano por habitante fue en 1987 inferior en un 25.1% a la de 1981; y la cosecha global de alimentos por persona fue en 1987 inferior en un 11.8% a la de 1981. Correlativamente, todas las grandes variables económico agrícolas han declinado abruptamente; la inversión pública y privada, el hato ganadero, el parque de tractores el crédito agrícola, etc.

---

juicios y procedimientos agrarios en que aquellos sean parte, se tomarán en cuenta sus prácticas y costumbres jurídicas en los términos que establezca la ley reglamentaria. (Constitución: 1992).

[7] (García: 1985).

[8] Stavenhagen señala que el cambio en las comunidades –hasta integrarse al capitalismo– se produce en un escenario de transformación permanente. (Alcántara: 1992).

[9] (CEPAL: 1989).

[10] (Calderón: 1988).

... Pero lo más preocupante es que las causas generadoras de estos fenómenos no limitan su acción a los años 1982-1987; están aún presentes, y amenazan a largo plazo la subsistencia de millones de campesinos, la alimentación de todos los mexicanos y la viabilidad general del desarrollo económico nacional[11].

Conforme a cifras estimadas por el banco de México, la contracción del producto agrícola entre los años de 1986 – 1988 ha sido sumamente severa: El P.I.B. agrícola declinó en un 4.96% en 1986, mientras que en 1987 creció apenas en un 0.7%, sin embargo, para marzo de 1988 hubo una nueva caída en un –0.54%. Comparativamente podemos establecer que conforme a estas cifras el producto agrícola per cápita cosechado en 1987 es inferior en aproximadamente 11.8% al de 1981[12].

«Tomando agregadamente los sectores agrícola y pecuario, la tasa compuesta de crecimiento anual medio fue del 4.7% en el período 1977-1981; mientras que en el período 1982-1987, la tasa de crecimiento pecuario fue del 1.1% inferior en 1.7% al incremento demográfico»[13].

Es en este marco de post modernización que el Estado mexicano ha establecido su nueva política agraria (nueva juridicidad agraria), todo ello conforme a los designios que años atrás, ya habían sido formulados por el banco mundial y que serán complementados con las nuevas disposiciones legales en materia de aguas, bosques y minas, entre otras.

Este proceso de modernización entre los diversos pueblos indios no necesariamente es o será homogéneo; las relaciones interétnicas y los procesos de articulación con la sociedad nacional guardan también un carácter diverso. Aunque consideramos que la tendencia principal ha sido la de colocar a las etnias en la depauperización – proletarización, manteniendo en la mayoría de los casos a sus territorios como reservas estratégicas del crecimiento capitalista.

La modernización, como política de Estado, puede constituirse en «alternativa» para los pueblos indios, solamente que sea analizada, discutida y asumida por los propios protagonistas. Una estrategia reconstructiva tanto de ejidos como de las «comunidades» permitiría que México, enfrentará los retos de la modernidad con la sabiduría de nuestros pueblos indios y campesinos. Los indios de México no son tan sólo herencia o folklore, sino que han constituído y constituyen una fuerza viva en la construcción del nuevo país.

2. PROBLEMATICA CON LA INFORMATICA

En este marco de modernización que se ha venido impulsando, entre otros aspectos la utilización de los ordenadores en el contexto de los pueblos indios de México.

---

(11) (Calva: 1988).
(12) (Banco de México: 1987).
(13) (Calva: 1988).

El hardware (las microcomputadoras) y el software (los programas para las computadoras), están orientados hacia las necesidades de la cultura occidental y, en particular, hacia las necesidades de las lenguas que utilizan una que otra variante del alfabeto romano (por ejemplo, inglés, francés y noruego).

Los hablantes de lenguas indias, es decir, sin una tradición literaria, todavía no tienen acceso a la tecnología computarizada, ni mucho menos a los procesadores de palabras en general.

Los ordenadores como tecnología no van a preservar a las culturas de los pueblos indios, pero sí pueden utilizarse para fomentar y apoyar el pluralismo cultural, así como proveer a los indios para que puedan editar y reproducir sus propios materiales didácticos.

Otra opción, del uso computacional, por los pueblos indios es imprimir sus propios folletos (en sus lenguas) por ejemplo acerca de como cultivar mejor el maíz, o registrar para generaciones futuras, las costumbres de la gente de hoy en día.

Es de justicia que los grupos étnicos de México, tengan los medios tecnológicos (sistemas corresponsales) ad hoc para su cultura.

El riesgo es precisamente que los usos computacionales deriven en ignorar a las minorías discriminadas, cuyo costo social sería muy alto ya que dichos sistemas computarizados están guiados por el discurso globalizador que desconoce la pluralidad social y cultural, llevando finalmente a una posible extinción de los pueblos indios.

BIBLIOGRAFIA

1.–Onceavo censo general de población y vivienda. Instituto Nacional de Estadística, Geografía e Informática; (INEGI), México 1990.

2.–I.N.E.G.I., Volumen Especial sobre hablantes de lenguas indígenas, México, p.p. 326-335.

3.–VALDÉZ LUZ MARÍA, El Perfil Demográfico de los Indios mexicanos, Ed. Siglo XXI, México 1988, p. 29.

4.–STAVENHAGEN RODOLFO, Derechos Indios en América Latina, Ed., el Colegio de México, México, 1988, p. 135.

DAES ERICA, Derechos del Pueblo Nativo en Boletín del Grupo Internacional de Trabajo, Vol. VI No. 5 Dinamarca 1988.

5.–CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Porrúa. México 1992, p. 15.

6.–Constitución op. cit. p. 3.

7.–GARCÍA ANTONIO, Reforma agraria y desarrollo capitalista en América Latina, Ed. U.N.A.M., México D.F., 1985, p. 14.

8.–ALCÁNTARA MERCADO, Gaceta UNAM de 15 de julio de 1992, p.18.

9.–CEPAL, Informe anual, año de 1989.

10–CALDERÓN JORGE, Cuadernos de Investigación Agraria, No. 39, División de Est. de Postgrado, F. de Economía UNAM, 1988.

11–CALVA JOSÉ, Crisis agrícola y alimentaria en México 1982-1988, Ed. Fontamara, México 1988, p. 9.

12–BANCO DE MÉXICO, Indicadores Trimestrales de la flotividad productiva. Variación anual 1986-1987, Méx. 1987.

13–Calva op. cit., p. 12.

«"Informática y derecho" como asignatura para informáticos»

FERNANDO GALINDO AYUDA(*)

Profesor titular de Filosofía del Derecho, Moral y Política. Seminario de Informática y Derecho de la Univ. de Zaragoza (ESPAÑA)

INTRODUCCION

El fundamento para la impartición de una asignatura como la que aquí se propone, que, como su título expresa, pretende establecer relaciones entre actividades humanas diferentes, como son las de los informáticos, vinculadas predominantemente al desarrollo de tecnologías o instrumentos técnicos adecuados para construir programas, y las de los juristas, cuya razón de ser es la resolución justa de conflictos concretos utilizando textos jurídicos o criterios generales, reside inmediatamente en la necesidad, expresada por la promulgación de textos legales destinados a la protección de datos personales tratados automáticamente y de códigos morales para informáticos, de que las actividades de los informáticos están guiadas, como sucede con las actividades de los juristas, por el respeto a las particularidades de las aplicaciones que realicen, y más en concreto a los valores y criterios que las regulan, reconocidos por una determinada sociedad.

Dicha necesidad es muestra de otra de mayor magnitud, que se expresa por la circunstancia de que en la sociedad mundial de los noventa se ha hecho realidad en prácticamente todos los países un fenómeno que con anterioridad

(*) Este trabajo ha sido financiado parcialmente por la CICYT, proyecto PB90-0582.

sólo se anunciaba: el uso habitual de las tecnología de la información y la comunicación por empresas, oficinas de la Administración y ciudadanos en general. La implantación ha sido realizada por acciones desarrolladas aislada o conjuntamente por empresarios, gobernantes y técnicos. Lo cual comporta que, aunque la responsabilidad de su concreción material haya recaído en los informáticos, denominado con este término, luego se harán mayores previsiones, a los expertos en el desarrollo y la puesta en acción de las mencionadas tecnologías, en general ya no sea posible una consideración exclusivamente técnica de ellas. Siempre ha de tenerse en cuenta su impacto social, aun cuando los datos manejados por las aplicaciones no sean de carácter personal.

Ello es debido a que la expansión de dichas tecnología en prácticamente todos los ámbitos de la vida [1] están produciendo un cambio de los hábitos sociales. Hasta el punto de que si bien las acciones concretas de quienes las utilizan son responsabilidad suya y en cuanto tales están caracterizadas por ser obra de sus convicciones o creencias, en buena medida están afectadas por las peculiaridades generales de las aplicaciones utilizadas, y en este sentido por los fines o valores en los que creen aquellos que han participado en su diseño. Como luego veremos sobre todo por los fines o valores en los que creen los que disponen el uso de la técnica: empresarios y gobernantes. Esta afirmación está en contra de lo que hasta estos momentos se ha venido reconociendo: hasta ahora se ha realizado tan sólo una consideración general y abstracta de las tecnología de la información y la comunicación. Cuando se ha entrado a valorarlas, se las ha criticado o ensalzado en su totalidad, sin caer en la cuenta de que ni la una ni la otra son posiciones correctas. Es más adecuado decir que, como en todas las actividades humanas, es posible un uso correcto y un uso incorrecto de las aplicaciones. Ello depende de la voluntad política de quienes las proyectan, encargan o utilizan.

Parecería con ello, que los valores en los que creen los técnicos que las han diseñado no influyan en el desarrollo de las aplicaciones o productos. Según creencia generalizada su mediación es meramente técnica, y en cuanto tal guiada por las características «objetivas» de los métodos e instrumentos que integran la ciencia o técnica de la informática o la computación. Puede decirse que ellos serían los buenos de la película, o la mano inocente instrumentalizada por otros: empresarios o gobernantes y usuarios. Esta convicción está cuestionada por lo siguiente.

La caracterización valorativa de las acciones de los informáticos se muestra en varias de sus facetas. Por un lado cabe tener en cuenta las valoraciones que efectúan los informáticos cuando actúan profesionalmente, ligán-

[1] Por medio de las técnicas de inteligencia artificial lo automatizado en cualquier ámbito es la aproximación que determinadas personas –expertos– realizan a los datos que dan cuenta de cualquier realidad. Aunque la aplicación verse, por ejemplo, sobre datos relativos a yacimientos de minerales, su fin principal es la transmisión del conocimiento sobre los mismos que han sido acumulados a lo largo de un periodo de su vida por determinados especialistas.

dose a través de contratos con uno u otro responsable de la realización de programas, valores incluidos. Otro aspecto es el relativo a la elección que realizan de una u otra técnica para desarrollar una aplicación lo que tiene su importancia porque no es indiferente el uso de uno u otro tipo de herramienta, dado que ello influye en la construcción de prototipos, en el desarrollo de la aplicación y en su implantación pues bien, en dicha elección influyen valores. Otra faceta es la referida al tipo de aproximación hacia la realidad social que efectúan los técnicos que construyen las aplicaciones o programas. Esta última cualidad profesional de los informáticos es la que aquí nos interesa especialmente, una vez que pretendemos ir al fondo del problema y, como veremos, el estudio de esta operación realizada por todos los informáticos en el ejercicio de sus actividades, lo permite.

Por todo lo cual se hace imprescindible la enseñanza a los informáticos por parte de los expertos en valoraciones o criterios sociales de conducta, los juristas, del marco de sus actividades: en concreto las características, consecuencias sociales y políticas de las mismas, así como las de las leyes y pautas morales de conducta que las regulan.

Aquí se va a ilustrar todo lo dicho a la vez que se muestra lo siguiente. En primer lugar (I), nos fijamos en qué es lo que caracteriza a los informáticos como profesionales. En definitiva qué son y qué hacen; en concreto el tipo de actividades que realizan en el ejercicio de su profesión.

En segundo lugar (II), señalaremos, en forma ejemplar, algunas pautas o criterios fundamentales de conducta profesional que se les propone socialmente, atendiendo tanto a lo que prescriben las leyes como los usos sociales, y en consecuencia los criterios y pautas de conducta a los que están obligados.

Finalmente elaboraremos una síntesis de la fórmula más adecuada para presentarles tanto las conductas que realizan y han de realizar, cuanto las reglas que han de cumplir, a través de la impartición de una asignatura denominada «Informática y Derecho», en las licenciaturas y diplomaturas donde se enseñen técnicas informáticas, a cuyo contenido nos referimos al final del trabajo (III).

I. ACTIVIDADES DE LOS INFORMATICOS

No es tan fácil definir qué son los informáticos o a quiénes cabe otorgar este atributo. Y es importante determinarlo porque en su función han de ser establecidos criterios de conducta, reglamentaciones y una enseñanza adecuada de unos y otras.

El problema viene del reciente origen de la profesión del informático, que es una profesión nueva, más nueva que el ordenador cuyos orígenes están situados en la segunda guerra mundial, todavía no estabilizada, entre otras razones por el mismo rápido desarrollo de la tecnología. Por ello no hay todavía suficiente experiencia académica: buena parte de los informáticos

actuales han sido formados en otras profesiones: son físicos, ingenieros, e incluso abogados o médicos, por ejemplo. En buena parte de las ocasiones son autodidactas en el manejo de programas y máquinas.

Por otro lado: existe una gran confusión. Se considera que son informáticos tanto el programador o el analista cuanto el vendedor de software o hardware de una empresa, siendo que, obviamente, esas son personas que realizan funciones distinas a las propias del informático. En la práctica social se observa, además, que hay quien considera informáticos a los profesionales de otras materias o especialidades, quienes únicamente son meros usuarios de las nuevas tecnologías, que han adquirido con su práctica suficientes conocimientos como para manejar un programa de tratamiento de textos o la jerga informática mínima...

¿Cabe considerar a todos ellos informáticos?, la verdad es que aunque dichos usos están comunmente admitidos no parece conveniente tomarlos como punto de referencia. Además. No es fácil encontrar lo común a todos los tipos profesionales anunciados; tal vez lo sea manifestar que reside en la experiencia en el manejo de las nuevas tecnologías. Con ello la solución al problema residiría en salir fuera de él: caracterizar absolutamente a las nuevas tecnologías. De esta forma se obtendrían las características de los informáticos y de sus actividades. Pero ello es insuficiente porque así también por ejemplo, cabe caracterizar a la sociedad actual en su totalidad, una vez que es difícil pensar en alguien que esté al margen de manejar o ser manejado por un ordenador en cierta forma. En definitiva estos son planteamientos generales y sobre planteamientos generales no cabe tomar posiciones. Para argumentar, como para razonar, es preciso abordar un punto de partida concreto o un problema.

En este sentido una fórmula adecuada para explicar a los informáticos como profesionales, puede ser la de tomar como punto de referencia la consideración de las características de una profesión establecida como la de los juristas, y a partir de sus cualidades, atendiendo a la diferencia de funciones entre unos y otros, establecer las notas peculiares de la profesión de informáticos. Ello es lo que realizamos a continuación.

Como decíamos al comienzo de este trabajo, la profesión de jurista está caracterizada fundamentalmente por la realización de justicia, resolviendo conflictos ocurridos en una sociedad, en la cual el profesional ha de colaborar con otros profesionales aplicando las leyes con el fin de atribuir a cada uno lo suyo. Esta resolución concreta de conflictos se produce mediante la puesta en práctica, a través de las técnicas jurídicas correspondientes guiadas por el peculiar sentido de justicia del profesional que resuelve el problema [2] some-

[2] Recuérdese que el sentido de justicia del profesional que ejerce en el Estado de Derecho está conformado por sus principios fundamentales, reconocidos en los textos de la Constitución y el resto del ordenamiento, que obligan a los juristas a motivar, utilizando las fuentes jurídicas en todas las actuaciones.

tido a las leyes, de distintas actividades. En estos momentos las más importantes son: interpretación y aplicación del Derecho, construcción de normas y de dogmas, y acceso a los textos jurídicos.

Desde otra perspectiva, la de la dependencia funcional, ha de decirse que la profesión de jurista se caracteriza por su realización en buena medida sin atender a mandato alguno: el jurista actúa como abogado de forma autónoma, y aun cuando esté integrado en la Administración de Justicia o en la gubernamental es independiente en el ejercicio de sus funciones, estando capacitado para resolver problemas de su competencia en su totalidad.

Con los antecedentes hasta aquí recogidos: ¿cuáles podemos decir son las actividades propias de los informáticos?

A primera vista, las actividades de los informáticos son distintas de las de los juristas. Estos, por su obligación de motivar, actúan siempre guiados por el interés principal de alcanzar la solución justa/democrática de conflictos o casos concretos, mientras que los informáticos actúan, también ante problemas concretos, pero con el fin principal de perfeccionar técnicas industriales, en este caso las propias de la programación. En cierta forma cabría decir que los informáticos persiguen un fin instrumental o de carácter teórico: conocer más; mientras que el de los juristas es práctico: hacer justicia o la paz. Los informáticos necesitan de un complemento: alguien ha de trazar –y poner los medios adecuados– el fin práctico de sus actividades, mientras que los juristas son autosuficientes: han de tratarse a sí mismos dicho fin. El fin a los informáticos les viene señalado por la empresa o el Estado que los contrata para programar.

Congruentemente con ello la formación del informático está centrada exclusivamente en el conocimiento de fundamentos teóricos y técnicas básicas o auxiliares: matemáticas o computación, programación, técnicas de investigación operativa, electrónica... La del jurista, en cambio, está dirigida a habituar al profesional en el manejo de las técnicas jurídicas en los distintos papeles que le corresponde interpretar socialmente: abogado especialmente, en países continentales; juez en Alemania y países anglosajones.

Todo ello parece proponer que las actividades típicas del informático son meramente técnicas: la construcción de aplicaciones o programas, o lo que es lo mismo la realización del análisis de determinada realidad social, utilizando la metodología pertinente, a efectos de reducir su complejidad por medio de la construcción de la oportuna formalización y la confección de la programación necesaria para resolver un problema utilizando los lenguajes adecuados. Esta afirmación está confirmada por otro uso de la expresión «informáticos» que sucede en la práctica: con frecuencia se dice de las actividades de los informáticos que son propias de ingenieros. Si la ingeniería como expresa el Diccionario, es el «arte de aplicar los conocimientos a la invención perfeccionamiento o uso de la técnica industrial en todas sus deter-

minaciones», no parece desencaminada dicha cualificación. De hecho en España es la denominación propia de los informáticos, en recientes normas en las que se establecen las Directrices propias de los planes de estudios conducentes a la titulación de «Ingeniería informática».

Los informáticos son, pues, ingenieros. Pero ¿qué tipo de ingenieros?, sin duda expertos en técnicas de programar. Programar, dice el Diccionario, es «preparar los datos indispensables para obtener la solución de un problema mediante una calculadora electrónica». Siguiendo las categorías clásicas se puede decir que hay problemas matemáticos, científicos y sociales [3]. Y por lo mismo cabría decir que existen programas matemáticos, científicos y sociales. Admitiendo inicialmente el sentido actual de la clasificación ha de decirse que en la práctica de la programación nunca ha sido adecuada: los programas de ordenador siempre se han realizado contando con que han de ser utilizados por hombres. Ello todavía sucede más con los más recientes programas desarrollados, que se fundamentan en la denominada inteligencia artificial. Por ello, los informáticos que elaboran los programas... ¿no pueden ser considerados ingenieros sociales?

Por lo hasta aquí reseñado bien puede aceptarse que los informáticos son ingenieros sociales, cuya labor principal consiste en seleccionar los datos de la realidad que consideren indispensables para obtener la solución de un problema mediante un ordenador. Ello supone reconocer que hay razones suficientes para acudir, con el fin de explicar esta actividad, a las propuestas de la filosofía del conocimiento.

Es inexcusable en este sentido referirnos a que las reflexiones filosóficas de carácter liberal vinculadas a los fundamentos kantianos [4] o

---

[3] KANT, M., *Fundamentación de la metafísica de las costumbres,* México, Editorial Porrúa, 1986, p. 15: «La antigua filosofía griega dividíase en tres ciencias: la física, la ética y la lógica. Esta división es perfectamente adecuada a la naturaleza de la cosa y nada hay que corregir en ella... Todo conocimiento racional, o es material y considera algún objeto, o es formal y se ocupa tan sólo de la forma del entendimiento y de la razón misma, y de las reglas universales del pensar en general, sin distinción de objetos. La filosofía formal se llama lógica; la filosofía material, empero, que tiene referencia a determinados objetos y a las leyes a que éstos están sometidos, se divide a su vez en dos. Porque las leyes son, o leyes de la naturaleza, o leyes de la libertad. La ciencia de las primeras llámase física, la de las segundas, ética; aquélla también suele llamarse teoría de la naturaleza, y ésta, teoría de las costumbres». La posibilidad de realizar una física de las costumbres por medio de la sociología fué explicada con posterioridad por Comte.

[4] KANT, M., *Fundamentación de la metafísica de las costumbres,* México, Editorial Porrúa, 1986, p.28: «Para saber lo que he de hacer para que mi querer sea moralmente bueno, no necesito ir a buscar muy lejos una penetración especial. Inexperto en lo que se refiere al curso del mundo; incapaz de estar preparado para los sucesos todos que en él ocurren, bástame preguntar: ¿puedes querer que tu máxima se convierta en ley universal? Si no, es una máxima reprobable, y no por algún perjuicio que pueda ocasionarte a tí o algún otro, sino porque no puede convenir, como principio en una legislación universal posible; la razón, empero, me impone respeto inmediato por esta universal legislación, de la cual no conozco aún ciertamente el fundamento –que el filósofo habrá de indagar–; pero al menos comprendo que es una estimación del valor, que excede en mucho a todo valor que se aprecie por la inclinación, y que la necesidad de mis acciones por puro respeto a la ley práctica es lo que constituye el deber, ante el cual

«humeanos»[5] del conocimiento, ligadas a las notas universalistas del yo o de la conciencia individual, considerados como entes separados del mundo sensible, que entienden que es posible establecer reglas absolutas de conocimiento y por lo mismo, en cuanto obra suya, hipótesis de acciones de carácter general, dado que el mundo es cognoscible a partir de las categorías a priori comunes a todo sujeto individual, están cada vez más lejanas. Dichas reflexiones han sido moderadas por reflexiones de tipo comunitario o, mejor, relacional, que acotan el terreno de observaciones. Estas reflexiones en la mayor parte de las ocasiones sin dejar de lado los principios ilustrados de conocimiento, sitúan al sujeto y al objeto en un mismo terreno, interconectado, en el que la participación del uno por el otro es múltiple. Desde diferentes perspectivas se habla de comunicación intersubjetiva como fundamento o como último punto de referencia [6], de horizonte del conocimiento [7], incluso desde otra perspectiva, de vida práctica y virtuosa expresada en sentido aristotélico [8]. Lo cual significa que se ha venido a

---

tiene que inclinarse cualquier otro fundamento determinante, porque es la condición de una voluntad buena en sí, cuyo valor está por encima de todo».

[5] HUME, D., *Investigación sobre el conocimiento humano,* Madrid, Alianza, 1988, p.79: «De la misma manera que la naturaleza nos ha enseñado a usar nuestros órganos sin darnos conocimiento de los músculos y nervios por los cuales son movidos, igualmente ha implantado en nosotros un instinto que conduce al pensamiento por un curso que corresponde al que ha establecido entre objetos externos, aunque ignoremos los poderes o fuerzas de los que este curso y sucesión regular de objetos depende en su totalidad».

[6] APEL, K.O., *Teoría de la verdad y ética del discurso,* Barcelona, Paidós, 1991, p.144: «En cada praxis argumentativa puedo y debo suponer como cierto a priori (como certeza paradigmática del juego lingüístico irrebasable de la argumentación) que yo, por ejemplo, realizo necesariamente con un acto argumentativo una pretensión de verdad y de sentido, es decir, una pretensión de validez con referencia intersubjetiva, y que supongo, por principio, su realizabilidad en el sentido de la capacidad de consenso de la proposición afirmada. Esto significa que no debo ni puedo hacer depender de la certeza de esta suposición de una teoría, sólo hipotética, del acto de habla, o de la argumentación, o de la lógica. Pues sin la indicada suposición –esto es completamente cierto– no tiene ningún sentido querer establecer una teoría hipotética; y sin ella tampoco tiene sentido querer «entrar correctamente» en el «círculo hermenéutico» de la autoexplicación de la razón».

[7] VATTIMO, G., *Etica de la interpretación,* Barcelona, Paidós, 1991, pp.61s: «En general, que el pensamiento se vuelva a la hermeneútica para reencontrar la historicidad y esencialidad de los contenidos que el estructuralismo había olvidado, se explica por el peso determinante que la teoría de la interpretación, ya desde su clásica formulación en Gadamer, confiere a la Wirkungsgeschichte y al wirkungsgeschichtliches Bewusstsein; la interpretación no es ninguna descripción por parte de un observador «neutral», sino un evento dialógico en el cual los interlocutores se ponen en juego por igual y del cual salen modificados; se comprenden en la medida en que son comprendidos dentro de un horizonte tercero, del cual no disponen, sino en el cual y por el cual son dispuestos. Mientras que el pensamiento estructural tenía por telos la clarificación y la toma de posesión por parte de la conciencia observante, de órdenes articulados de acuerdo con reglas, el pensamiento hermenéutico pone el acento en la pertenencia de observante y observado a un horizonte común, y en la verdad como evento que, en el diálogo entre los dos interlocutores, «pone en obra» y modifica, a la vez tal horizonte. En el juego que, en Verdad y Método de Gadamer, es el modelo del acaecer de la verdad hermenéutica, los jugadores son siempre a su vez jugados; y la conciencia, en cuanto históricamente determinada, no puede ya alcanzar la perfecta autotransparencia».

[8] MACINTYRE, A., *Tras la virtud,* Barcelona, Crítica, 1987: «Los personajes esenciales

trasladar el objeto de la reflexión filosófica desde los sujetos y los objetos a la relación entre ambos, estudiándose históricamente, en un primer momento el lenguaje, después la acción que establece el marco de la participación y del conocimiento. Ahí encuentran su último fundamento las expresiones filosóficas práctica, filosofía de la argumentación e historia de la ciencia, denominadores habituales de la discusión sobre el conocimiento en estos momentos.

Estas actitudes son consecuencia de la asunción de las siguientes críticas sobre la reflexión filosófica del XIX y el XX, que han sido resumidas recientemente en el seno de la discusión modernidad–postmodernidad:

«a) Quien, al centrar su interés en la relación consigo mismo que caracteriza al sujeto cognosciente, se decidía elegir la autoconciencia como punto de partida de su análisis, tenía que haberselas ya desde Fichte con la objeción que la autoconciencia no puede considerarse en absoluto un fenómeno originario, pues la espontaneidad de la vida consciente escapa justo a aquella forma de objeto en la que, empero, tendría que ser subsumida en cuanto el sujeto cognoscente se vuelve sobre sí para apoderarse del sí como de un objeto. Esta coerción que los conceptos básicos elegidos ejercen y que obliga a la objetivación y a la autobjetivación viene sirviendo también desde Nietzsche de blanco de una crítica a la forma de pensamiento que tiene por meta apoderarse de objetos y a la razón instrumental...

b) Desde Frege la lógica y la semántica dieron un golpe a esa concepción articulada en términos de teoría del objeto, que resulta de la estrategia conceptual de la filosofía de la conciencia. Pues son sólo siempre objetos, en palabras de Husserl: objetos intencionales, a lo que pueden dirigirse los actos del sujeto que juzga, actúa y tiene vivencias. Pero esta concepción del objeto representado no hace justicia a la estructura proposicional de los estados de cosas a que nos referimos (gemeinten) y que reflejamos en enunciados.

c) Además el naturalismo pone en duda que sea posible partir de la conciencia como base, como algo incondicionado y originario: habría que conciliar a Kant con Darwin. Más tarde, con las teorías de Freud, Piaget y Saussure, ofreciéronse categorías «terceras» que acabaron socavando el dualismo conceptual con que operaba la filosofía de la conciencia. A través de las categorías de cuerpo susceptible de expresarse, de comportamiento, de

---

del guión dramático de la modernidad, el experto que conecta medios y fines de manera valorativamente neutra y el agente moral que es a la vez nadie en concreto y cualquiera que no esté mentalmente disminuido, no tienen contrapartida auténtica en el esquema de Aristóteles o dentro de la tradición clásica. En realidad, es difícil postular la exaltación de la pericia burocrática en cualquier cultura donde la conexión entre la inteligencia práctica y las virtudes morales esté firmemente establecida»(pp. 195s). «Mi conclusión es muy clara: de un lado, que todavía, pese a los esfuerzos de tres siglos de filosofía moral y uno de sociología, falta cualquier enunciado coherente y racionalmente defendible del punto de vista liberal-individualista; y de otro lado, que la tradición aristotélica puede ser reformulada de tal manera que se restaure la inteligibilidad y racionalidad de nuestras actitudes y compromisos morales y sociales». (p. 318)

acción y de lenguaje pueden introducirse relaciones con el mundo, en las que ya está inserto el organismo socializado, el sujeto capaz de lenguaje y de acción antes de poder referirse a algo en el mundo en términos objetivantes... sólo con el giro lingüístico han encontrado tales reservas [las efectuadas con respecto a las consideraciones filosóficas liberales] un sólido fundamento metodológico. Este giro se debe al abandono, marcado ya por Humboldt, de la concepción tradicional según la cual el lenguaje ha de entenderse conforme al modelo de la asignación de nombres a objetos y como un instrumento de comunicación que permanece externo al contenido del pensamiento... esta nueva concepción de lenguaje [lengüaje ligado al sujeto, en su contexto], de cuño trascendental, cobra relevancia paradigmática ante todo por la ventaja metodológica que supone frente a una filosofía del sujeto que ha de apelar un acceso introspectivo a los hechos de conciencia...» [9]

Expresión lingüística que precisa de complementos porque: «La descripción de entidades que aparecen en el interior del espacio de representaciones de la corriente de vivencias, no logra liberarse de la sospecha de no ser más que puramente subjetiva, ora se apoye en la experiencia interna, en la intuición intelectual, o en la evidencia inmediata. La validez intersubjetiva de las observaciones sólo puede venir asegurada por la práctica experimental, es decir, por una transformación regulada de las percepciones en datos. Una objetivación similar es la que parece lograrse cuando el análisis de las representaciones y pensamientos se emprende recurriendo a los productos gramaticales con cuya ayuda son expresados. Las expresiones gramaticales son algo públicamente accesible, en ellas pueden leerse estructuras sin necesidad de referirse a algo meramente subjetivo. El modelo que representaron la matemáticas y la lógica hizo el resto, para que la filosofía se viera remitida con carácter general al ámbito objetual público que representan las expresiones gramaticales, Frege y Peirce marcan el punto de inflexión» [10].

Tras esta situación se produjo el denominado giro pragmático, dado por la filosofía del lenguaje con el fin de superar las abstracciones estructuralistas, en las que desembocó dicha filosofía por la expansión del uso de la semántica o la semiótica. Se vino a caer en la cuenta de que...«las operaciones trascendentales en modo alguno se han retraido como tales a los sistemas gramaticales de reglas, antes la síntesis lingüística es el resultado de operaciones constructivas de entendimiento que se efectúan en las formas de una intersubjetividad discontinua...»[11].

Por ello ahora se entiende que conocer es lo mismo que construir propuestas sobre actos limitados: sobre acciones realizadas o realizables en el mundo por sujetos concretos, dirigidos a otros, con el fin de entenderse o

---

[9] HABERMAS, J., Pensamiento postmetafísico cit. pp. 55s.
[10] Ibidem
[11] Ibidem pp. 58s

comunicarse. Ya no cabe realizar grandes propuestas, de carácter inmensurable, se entiende que tales propuestas están vacías. El conocimiento tiene lugar por medio de acciones comunicativas, en lugar de acciones estratégicas: «Como la acción comunicativa depende de una utilización del lenguaje orientada al entendimiento, ha de satisfacer condiciones más estrictas. Los actores implicados tratan de sintonizar cooperativamente sus planes de acción en el horizonte de un mundo de vida compartido y sobre la base de interpretaciones comunes de la situación. Están además dispuestos a alcanzar esos fines indirectos que son la definición de la situación y la sintonización de fines a través de procesos de entendimiento sostenidos en el papel de hablantes y oyentes es decir, por la vía de una persecución sin reservas de fines ilocucionarios. Ahora bien, por su propia estructura el funcionamiento del entendimiento lingüístico consiste en que los participantes en la interacción se ponen de acuerdo sobre la validez que pretenden para sus actos de habla o, correspondientemente, tienen presente los desacuerdos que constatan. Con los actos de habla se entablan pretensiones de validez susceptibles de crítica, que tienen por meta un reconocimiento intersubjetivo. La oferta que un acto de habla comporta cobra la capacidad de establecer vínculos porque el hablante al entablar una pretensión de validez garantiza también y de forma digna de crédito, que en caso necesario podrá desempeñar también dicha pretensión con la clase correcta de razones. La acción comunicativa se distingue, pues, de la acción estratégica en el respecto de que el buen suceso en la coordinación de la acción no se basa en la racionalidad con respecto a fines de los distintos planes de acción individuales, sino en la fuerza racionalmente motivadora que tienen las operaciones de entendimiento, en una racionalidad, por tanto, que se manifiesta en las condiciones a que está sujeto un acuerdo comunicativamente alcanzado.»[12].

Esta reflexión pone de manifiesto que todo conocimiento ha de tomar como objetivo inicial no tanto la construcción de formalizaciones correctas o frases bien formadas, cuanto estructuras momentáneas de la realidad, consideradas ya no desde una perspectiva individualista, sino desde la perspectiva del entendimiento. Lo cual significa que la reflexión sobre el conocimiento, extendida también al conocimiento sistémico [13], se hace desde la perspectiva de tomar como orientación la de propiciar se hagan explícitas para con acciones concretas, a través de todos los procedimientos (científicos y filosóficos), todas las peculiaridades de la comunicación [14]

---

[12] Ibidem: p. 74

[13] MATURANA, H., «Biology of cognition (1970)» en, MATURANA, H., VARELA, F., (eds), Autopoiesis and Cognition: The Realization of the Living, Dordrecht, Kluwer, 1980, pp. 2-62

[14] «La argumentación no es un porcedimiento de decisión que acabe en resoluciones sino un procedimiento de solución de problemas que conduce a convicciones. Naturalmente, la disputa argumentativa sobre la pretensión de verdad de los enunciados asertóricos, o sobre la pretensión de rectitud de los enunciados normativos puede quedar en tablas, de suerte que no se produzca acuerdo alguno, entonces, for the time being, habrá que dejar abierta la cuestión, pero con la conciencia de que sólo una de las partes puede tener razón. Ahora bien, en los discursos

También por ello, se cuenta con los criterios o prejuicios sociales que se utilizan por los sujetos en sus acciones, porque el único objeto de la acción comunicativa es el entenderse. Ha de tenerse en cuenta, con Habermas, que: «Los ámbitos simbólicamente preestructurados, lingüísticamente constituidos que son la cultura y la sociedad exigen un terreno intermedio entre la investigación y el pensamiento, entre la racionalidad de la objetivación y la de la vida consciente». [15]

Con lo cual ha de reconocerse que no hay tanta lejanía como parecería inicialmente entre la actitud profesional de los juristas y la de los informáticos. Si para los primeros decíamos que su actividad profesional está guiada por el acuerdo concreto para con los valores mayoritarios expresados en criterios o reglas: en definitiva la satisfacción de la virtud de la justicia, también la actuación de los informáticos necesita estar guiada por criterios o valores mayoritarios.

Así pues, tras lo dicho ha de admitirse que incluso la mera reconstrucción de los datos sociales a efectos de constituir el sistema inicial: el punto

---

prácticos puede que ocurra que el tema de que se trataba resulte no ser en absoluto de naturaleza moral. Puede que se trate de una cuestión ético-existencial que afecte a la autocomprensión de determinadas personas o de un determinado colectivo; entonces la respuesta, por racional que sea, sólo puede ser válida relativamente a mi objetivo, o nuestro objetivo, de una vida feliz o de una vida no fallida, y no puede pretender tener un carácter universalmente vinculante. Pero quizá pueda tratarse también de la cuestión pragmática del equilibrio o armonización de intereses contrapuestos, no susceptibles de universalización; entonces, a lo más que los participantes pueden aspirar es a llegar a un compromiso «fair» o aceptable. De modo que, en el ámbito de la praxis, el fracaso de los intentos de argumentación puede tener también el sentido de que lo que en realidad estábamos desarrollando no era un discurso de tipo moral, sino un discurso relativo a la compresión individual de nosotros mismos, o una negociación.

También la formación parlamentaria de la voluntad común encierra un núcleo racional; pues las cuestiones políticas son susceptibles de un tratamiento discursivo, así desde puntos de vista empíricos y pragmáticos, como desde puntos de vista morales y éticos, mas estos procesos jurídicamente institucionalizados de formación de opinión están programados para que acaben en una toma de decisiones a plazo más o menos fijo. El orden del día combina una formación de la opinión, orientada, por tanto a la verdad, con la formación de una voluntad colectiva, atenida a la regla de la mayoría. Mas desde el punto de vista de una teoría del discurso que no tiene más remedio que desmenuzar tales procedimientos a la búsqueda de lo que, pese a todo, hayan de haber de racional, la regla de la mayoría ha de mantener una interna referencia a una búsqueda cooperativa de la verdad. Conforme a su propia idea, una decisión mayoritaria sólo puede (debe) producirse en condiciones discursivas tales, que su resultado pueda tener a su favor la presunción de racionalidad. El contenido de una decisión obtenida conforme a los procedimientos establecidos tiene que poder considerarse resultado racionalmente motivado, aunque falible, de una discusión provisionalmente interrumpida a causa de la necesidad de decidir. Por tanto, hay que distinguir bien entre el discurso como procedimiento de formación del juicio moral y ético y el procedimiento jurídicamente institucionalizado de tomas de decisiones políticas (por más que éstas vengan y tengan que venir mediadas por discursos)». HABERMAS, J., La necesidad de revisión de la izquierda, Madrid, Tecnos, 1991, pp 180-182. Ha de tenerse en cuenta que el ejemplo de la elaboración de la ley es referencia para la creación de cualquier tipo de disposiciones jurídicas, una vez que, en el Estado de Derecho, en todas ellas rigen los principios democráticos a través de la normativa que regula procedimientos y procesos.

[15] HABERMAS, J., *Pensamiento postmetafísico* cit. p. 272

de partida de la labor del informático, nunca sucede en abstracto; depende de la interacción que se produce entre el sujeto y el objeto. Dicho de otra forma: de los prejuicios o valores en los que cree el informático, de los del que encarga su trabajo –principalmente–, en la medida de lo posible de las opiniones del usuario y de las características del objeto: el fin a realizar por el programa a construir. En definitiva importan en su construcción los criterios que están presentes y son reconocidos como tales por los integrantes de una determinada sociedad. El informático, por ello, ha de ser consciente de que conoce y actúa como intermediario de un determinado conjunto de mundos de vida o valoraciones que configuran el problema para el que ha de realizar un programa. No en vano, por ejemplo, cualquier informático sabe que a la hora de actuar puede seleccionar una metodología de entre todo un conjunto de metodología que ofrecen perspectivas muy diferentes de la realidad social en virtud de cual sea el acuerdo valorativo para el caso concreto. La pluralidad de metodología depende de la heterogeneidad de técnicas existentes, y también sin duda alguna, de la pluralidad de convicciones sociales existentes. [16]

De ahí hayamos expresado que en lo que respecta al conocimiento y a la acción tanto el informático como el jurista, como cualquier otro profesional, están caracterizados por actuar valorativamente [17]. Salvadas las distancias, la diferencia entre uno y otro queda limitada al hecho, sin duda relevante, de que si bien el jurista ha de ayudar a resolver casos conflictivos concretos en los que los implicados son pocos, siendo por ello participados de forma inmediata por un cálculo reducido de personas, en cambio el informático ha de resolver problemas de alcance más general. El informático ha de estudiar datos de la realidad de dimensión suficiente como para construir programas en los que están implicados directa o indirectamente grupos de población numerosos y en cierta medida indeterminados. Por ello si la actitud del jurista ha de ser personalista, la del informático, en cambio, ha de ser generalista. De ahí que el tipo de reflexión que interesa a uno y a otro son distintas: más bien sociológica en el caso del informático, filosófica en el caso del jurista. La teoría de sistemas interesa al informático en mayor medida. La de la argumentación al jurista. La teoría de la acción comunicativa, en cambio, a ambos.

Estas propuestas pueden parecer teoréticas, e incluso, desde otra perspectiva, retóricas al no iniciado. A efectos de despejar esta duda me remito al siguiente apartado en el que se narra cómo en el fondo estas apreciaciones,

---

[16] HIRSCHHEIM, R., KLEIN, H.K., «Four Paradigms of Information Systems Development», Communications of the ACM,vol. 32, 1989, pp. 1207-1209.

[17] Ha de tenerse siempre presente, pese a todo, la radical diferencia existente entre las técnicas utilizadas por el jurista y el informático: El primero se fundamenta en la ciencia del derecho o dogmática, mientras que el segundo lo hace en los fundamentos de la física y la matemática.

entre otras, [18] son la explicación que justifica la proliferación existente de leyes y códigos morales que se preocupan por fijar a partir de valores reconocidos socialmente, bajo la amenaza de sanción administrativa, penal y moral (económica), el ámbito del conocimiento y de las actividades a realizar por el informático y por el que le encarga sus programas. Señalan su horizonte. Por ello ya podemos decir que las actividades del informático han de estar guiadas por la justicia, o lo que es lo mismo han de ser justificadas o motivadas no tan sólo por criterios técnicos, sino, también por criterios o valores prescritos por las leyes o por los códigos morales de conducta.

II. CRITERIOS DE CONDUCTA

En general los criterios de conducta por los que ha de regirse cualquier profesional, están integrados por los reconocidos como tales en un determinado contexto: el que forman los miembros de los grupos profesionales que lo componen. También por los jurídicos, que son, fundamentalmente, los recogidos en los textos legales, prescritos a los profesionales bajo amenaza de sanción penal o administrativa en caso de incumplimiento.

Los primeros son propiamente criterios morales. Dependen del mundo de vida: de la naturaleza de la profesión de sus consecuencias, y las convicciones admitidas socialmente. Son los que por lo general tienen en cuenta los profesionales en su vida diaria. En escasa medida es precisa su regulación jurídica; en todo caso, como decíamos, son las asociaciones profesionales las que tienen competencia para establecerlos.

A diferencia de lo que sucede en otros terrenos, los informáticos están sometidos a los códigos de conducta profesional aprobados por Asociaciones profesionales de todo tipo: no exclusivamente informáticas; también por ejemplo, médicas o empresariales [19]. Han de estar registrados convenientemente y controlada su legalidad, en lo que respecta al tratamiento de los datos de carácter personal, por instituciones técnico-políticas como el Defensor de los datos. Otra peculiaridad de las actividades profesionales de los informáticos reside en que, a diferencia de lo que sucede con las actividades de otros ingenieros, la parte fundamental de las mismas, como es la relativa a la fijación del punto de partida de su actividad: la que podemos denominar la fijación de los hechos, en el caso del tratamiento automatizado de datos personales está regulada por disposiciones jurídicas. A semejanza de estas dispo-

[18] La justificación de las Leyes de Protección de Datos reside, sin duda alguna, en la vulneración de los Derechos Fundamentales, expresada incluso por acciones de protesta social, que se produce en aquellos lugares donde no han sido adoptadas.

[19] Anteproyecto de LORTAD, art. 31,1: «Mediante acuerdo sectorial o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular Códigos Tipo...2 Los Códigos Tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional...»

siciones las asociaciones de informáticos han extendido dicha exigencia a todas las aplicaciones. Veamos.

La más superficial observación a las leyes de protección del tratamiento automatizado de los datos de carácter personal, actualmente vigentes o a punto de ser aprobadas como es el caso de la española, permite observar que estas disposiciones establecen pautas de conducta destinadas a regular la actividad profesional de los informáticos en sus funciones de analizar la realidad y programar. La tendencia es creciente si se tiene en cuenta la previsión actual de promulgación de disposiciones europeas que se ocupan de establecer normas de seguridad para los sistemas de informaciónen general [20].

Para ser exactos diríamos que las normas de protección de datos, aparte, como es natural de a los ciudadanos y a los agentes jurídicos, destinatarios habituales de las leyes, están dirigidas: 1) a las autoridades especiales que se encargan de su observancia; 2) a los responsables del encargo de la construcción mantenimiento y difusión de los programas: empresarios y Estado, fundamentalmente Administración Pública; 3) a los informáticos. En efecto. Si nos fijamos en el contenido material de las disposiciones, observamos que la mayor parte de sus indicaciones están referidas a la recopilación de datos, o lo que es lo mismo a la actividad del análisis del sistema social constituido por los datos personales, y al tratamiento automatizado de los mismos, o a las características de los programas. Los datos y programas, por ello, han de ser manipulados atendiendo a determinados principios: los de las técnicas correspondientes, pero siempre dentro del marco concreto formado por los principios recogidos en los textos de los Derechos Humanos o Fundamentales. Instituciones de carácter técnico-político como son los Defensores de los datos se encargan de concretar técnico-políticamente dichos principios y velar por su observancia real.

Esto se comprueba observando el texto del Anteproyecto español de ley orgánica de tratamiento automatizado de los datos personales. Fijémonos en que de los siete títulos del anteproyecto cinco de ellos están destinados a señalar el ámbito de los sistemas y los programas: «Principios de la protección de datos», «Derechos de las personas», «Disposiciones sectoriales: ficheros de titularidad pública y ficheros de titularidad privada», «Movimiento internacional de datos» y «Agencia de protección de datos» [21]. Congruentemente con ello se dice en el artículo 2.1 al definir el ámbito de aplicación de la ley: «La presente Ley será aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carác-

[20] A ello se dedica la «Propuesta de Decisión del Consejo de las Comunidades Europeas en el ámbito de la seguridad de los sistemas de información», actualmente en periodo de discusión.

[21] El título primero está destinado a «Disposiciones generales» y el séptimo a «Infracciones y Sanciones»

ter personal registrados en soporte físico susceptible de tratamiento automatizado».

Los códigos morales de conducta para informáticos están de actualidad en estos momentos. Están construidos a partir de preferencias valorativas de todo tipo: fundamentalmente son, como el aire de los tiempos, de orientación utilitarista. También los hay guiados por la imparcialidad, desarrollados desde propuestas morales que ponen especial énfasis en la generalidad. También los hay comunicativos, caracterizados especialmente por reclamar el consentimiento de los interesados, ligados a las disposiciones jurídicas destinadas a la protección del tratamiento automatizado de datos personales. Aquí nos vamos a limitar a dar cuenta de algunas de las notas principales de esos tipos de códigos expresadas en algunos ejemplos. Un ejemplo de código utilitarista puede ser el propuesto por J. R. Wolfson, miembro de la Asociación estadounidense de distribuidores de seguridad (Securities Dealers) [22]. Este código se ocupa de establecer reglas de conducta destinadas a evitar conflictos de intereses. Acerca de su contenido ilustra lo siguiente. Se titula «código de responsabilidad de los profesionales de la informática». Consta de seis capítulos cuyos títulos son: «Un informático no perjudicará intencionalmente, ni por medio de un conflicto de intereses, a un usuario», «Un informático no perjudicará intencionalmente a cualquier otro informático o cualquier otra entidad informática», «Un informático no perjudicará a otros en el curso de sus actividades de Investigaciones y Desarrollo», «Los informáticos serán representantes válidos de ellos mismos», «Un informático será y permanecerá competente y cualificado» y «Un informático trabajará para promover el respeto de la profesión.»

Una muestra de código imparcial bien puede ser la última versión de código profesional propuesto por la Association for Computing Machinery (ACM) de Estados Unidos [23]. Se denomina «código de Etica y Conducta Profesional de la ACM». Tiene cuatro secciones dedicadas a lo siguiente. La primera propone consideraciones éticas generales; la segunda establece responsabilidades profesionales más específicas; la tercera prescribe normas a los profesionales que tengan una mayor responsabilidad, o bien en una empresa o institución, o bien en una corporación profesional como la ACM, y la cuarta establece reglas para promover el cumplimiento del código. Muestra de su contenido la dan los imperativos morales generales que, expresado todo ello en forma resumida, dirigidos a los miembros de la Asociación dicen: «Como miembro de la ACM... contribuiré al bienestar de la sociedad y de los hombres; evitaré perjudicar a otros; seré honesto y veraz; seré imparcial y no actuaré indiscriminadamente; respetaré los derechos de propiedad, inclu-

[22] WOLFSON, J.R., «A Conduct Code: An Echics Code With Bite», The Journal of Computing and Society, I (2), 1991, pp. 119-134.

[23] ACM Code of Ethics and Professional Conduct, Communications of the ACM, VOL. 35, 1992, pp.94-99.

yendo copyrights y patentes; confiaré en la propiedad intelectual; accederé a los sistemas de información y comunicación tan sólo cuando esté autorizado a ello; respetaré el derecho a la privacidad de otros; respetaré la confidencialidad del honor ajeno».

Como muestra del contenido de códigos de conducta profesional vinculadas a los principios establecidos en las leyes de protección de datos, caracterizadas, en cumplimiento del principio de autodeterminación y de participación por reclamar el consentimiento de los interesados, vamos a reseñar alguna de las normas aprobadas al efecto referidas a cuál debe ser su contenido mínimo, prescritas por una disposición reglamentaria de la Oficina del Registro de Protección de Datos inglés de septiembre de 1985, en ilustración del contenido de la Ley de protección de datos inglesa de 1984 [24].

En esta norma se dice que los códigos de práctica «deben establecer claras fórmulas de acciones prácticas a ser seguidas». En este sentido las reglas mínimas, a establecer en un código de práctica, deben referirse a lo siguiente: «Los individuos a los que sirve.– Los derechos de estos individuos en con relación a lo prescrito por los principios de la ley de protección de datos.– Los usuarios informáticos que encuentren pertinente el código de práctica.– Las obligaciones que tendrán estos usuarios con respecto a los principios de protección de datos.– El fin del código de práctica en lo relativo a los derechos y obligaciones que prescriba.– Las prácticas particulares incorporadas en el código; cómo se relacionan con los principios de protección de datos; cómo pueden ser incorporados por los usuarios informáticos en sus actividades profesionales dichas prácticas .– Cómo los individuos pueden ejercitar los derechos que emanen del código de práctica.– Cómo se expresa la adhesión a un código de práctica.– Las sanciones que pueden seguir de una infracción del código por un usuario informático adherido.– Qué usuarios informáticos están adheridos al código de práctica».

Los ejemplos podrían reiterarse dado que la experiencia en el mundo sobre protección de datos es muy extensa. Pero con la información hasta aquí suministrada ya se cuenta con datos suficientes como para satisfacer el objetivo inicial del presente trabajo: articular una asignatura de «informática y Derecho» a impartir en estudios informáticos.

III. CONTENIDO DE LA ASIGNATURA «INFORMATICA Y DERECHO»

Aquí se va a realizar una propuesta general, ha de tomarse como ideal.

De todas formas se van a tener en cuenta como horizonte formal las pautas recogidas en las Directrices comunes y propias de elaboración de los

[24] Office of the Data Protection Registrar, «Codes of Practice. A Preliminary Policy Statement (September 1985)», en CHALTON, S.. GASKILL, S., (eds), Encyclopedia of Data Protection, London, Sweet & Maxwell, 1988, p. 5001

planes de estudio aprobadas por el Consejo de Universidades españolas. Obviamente mayores concreciones a lo aquí establecido han de realizarse atendiendo a las necesidades docentes concretas de una Universidad en la que se decida la impartición de estas enseñanzas.

La denominación más adecuada para la asignatura en cuanto más comprensiva de lo que se va a explicar en ella es «Informática y Derecho». Otra posibilidad es «Etica profesional» o «Deontología profesional», pero con ello su ámbito resulta limitado: en todos los países, tras la aprobación de las leyes de protección de datos, las reglas de conducta para los informáticos están contenidas en mayor medida en textos jurídicos. Por otro lado las reglas éticas prescritas por asociaciones profesionales se remiten explícitamente a las leyes [25].

Fundamentalmente la propuesta está pensando en una asignatura a impartir en estudios que conduzcan a una licenciatura (o ingeniería) o una diplomatura en informática. También es posible su impartición en estudios de postgrado de carácter especializado como pueden ser los destinados a formar a los informáticos que se integren en la Administración Pública, dado que estos informáticos necesitan de una asignatura a propósito en virtud de su función. Es necesaria para informáticos que se integren en sectores profesionales que cuenten con códigos deontológicos especiales: documentalistas médicos es uno de los mejores ejemplos al respecto.

Difícilmente tendría entrada en otros estudios, al menos con carácter obligatorio, luego nos referiremos a ello.

En todo caso es una asignatura adecuada para el periodo final de los estudios: último año del primer ciclo, en el caso de Diplomatura; último año del segundo ciclo, en el caso de la Ingeniería o Licenciatura. En los cursos de postgrado también es conveniente su impartición al final de los mismos, una vez conocidas las peculiaridades de la profesión correspondiente.

Congruentemente con lo señalado antes, la disciplina ha de constar de las siguientes materias fundamentales: definición y características de las actividades profesionales típicas del informático, reseña y adiestramiento en su práctica de obligaciones morales y reseña y adiestramiento en su práctica de obligaciones jurídicas.

Por lo que respecta a la cantidad de materia a explicar o los créditos a atribuir a quien apruebe las evaluaciones pertinentes, ello, como es natural, dependerá entre otros datos, de la totalidad de créditos necesarios para obtener los títulos correspondientes, y fundamentalmente de la orientación general en lo que respecta a la carga de materia dada a la titulación por el centro que la imparta. No cabe establecer un término medio. En todo caso deberán ser

[25] Es el caso de la ACM. Ver ACM op. cit. p. 96

criterios de tipo teórico y práctico, repartidos en un porcentaje del cincuenta por ciento.

Es difícil afirmar absolutamente a cuál de las áreas de conocimiento establecidas le compete la docencia, dependerá de su concreción material y del tipo de licenciatura en el que sea admitida. Al menos, dado el contenido de la disciplina, ofrece pocas dudas su asignación a una de carácter jurídico.

Por lo que respecta al objetivo de la asignatura, éste ha de quedar centrado en hacer patente de forma práctica a informáticos cuáles son sus obligaciones profesionales y sus límites. Para ello se ha de atender tanto a lo señalado por las indicaciones hechas por la teoría del conocimiento, en especial la reflexión habida con respecto a teoría de sistemas, cibernética y acción comunicativa, cuanto a lo que establecen las prescripciones establecidas en leyes y códigos de conducta profesional.

Ni esta asignatura ni otra parecida han sido reconocidas como troncales por las Directrices de los planes de estudios aprobados por el Consejo de Universidades. En estos momentos se encuentran en fase de homologación planes de estudios de distintas Universidades. Por tanto, en todo caso la asignatura habrá de ser considerada asignatura propia de Universidad de carácter obligatorio, optativo o de libre configuración. Atendiendo a lo hasta aquí manifestado parece que la asignatura propuesta, con la cualificación que estime pertinente la respectiva Universidad, debería formar parte de planes de estudio conducentes al título de Ingeniero Informático [26] y los de Ingeniero Técnico en Informática de Gestión [27] e Ingeniero Técnico en Informática de Sistemas [28]. Es indispensable igualmente para las Diplomaturas de Estadística y Gestión y Administración Pública. Dependiendo de la configuración del plan de estudios puede interesar en la licenciatura en Matemáticas: especialidad Ciencias de la Computación.

Dado su contenido cabría fomentar su inclusión como asignatura de libre configuración para el curriculum de todos aquellos estudiantes que realicen estudios de alguna asignatura relacionada con informática.

Por lo que respecta a estudiantes de Derecho puede tener interés como asignatura optativa de segundo ciclo. Sobre todo en la parte de la materia concerniente a Derecho positivo. Es recomendable para los estudiantes que orienten su curriculum al trabajo en la Administración Pública. En lo relativo a las razones para su inclusión en los planes de estudios mencionados y su distinta cualificación todo ello queda explicado en los dos primeros apartados de este trabajo. Resumiendo podemos decir que, en definitiva, es indispensable a un informático, para poder realizar su propio trabajo profesional, conocer su profesión y las herramientas indispensables para mejor desenvolverla.

---

[26] Real Decreto 1459/1990, de 26 de octubre de 1990.
[27] Real Decreto 1460/1990, de 26 de octubre de 1990.
[28] Real Decreto 1461/1990, de 26 de octubre de 1990.

La asignatura se legitima porque estas herramientas están señaladas, en cierta medida, por los textos jurídicos y morales que delimitan la profesión de informático. El ejercicio responsable de la profesión exige tener conciencia de los criterios y valores por medio de los que se actúa en una determinada sociedad. La moral profesional del informático no se aprende simplemente por la práctica profesional, tiene las complejidades apuntadas, que han sido construidas a partir de costumbres políticas democráticas no explicadas por las diferentes disciplinas científicas y técnicas que integran mayoritariamente el plan de estudios.

Es difícil llegar a mostrar en una introducción como ésta un programa de la asignatura. Su concreción en forma de lecciones, dependerá del tipo de alumnado ante el que deba impartirse. Por ello no tiene mucho sentido extenderse al respecto. A modo de orientación no obstante, se señalan a continuación los grandes bloques temáticos de un hipotético programa dirigido a estudiantes de informática.

Tema I. Origen profesional de los informáticos: historia.–
Tema II. Los informáticos como ingenieros sociales.–
Tema III. Teoría de los sistemas sociales: principios.–
Tema IV. Teoría de la acción comunicativa.–
Tema V. Etica de la eficiencia: principios.–
Tema VI. Etica de la imparcialidad: principios.–
Tema VII. Etica comunicativa: principios.–
Tema VIII. Códigos deontológicos: principios básicos.–
Tema IX. Seguridad de los sistemas de información: técnicas principales.–
Tema X. Derecho informático, en especial la protección del tratamiento automatizado de datos personales.

Un programa no quedaría completo sin la reseña de una bibliografía básica que ilustrara sobre la orientación de la disciplina. Entre los muchos libros que pueden ser citados a estos efectos destacamos los siguientes:

BIBLIOGRAFIA

JOHNSON, D. G., Computer Ethics, Englewood Cliffs, NJ, Prentice Hall, 1985.–

LOSANO, M. G., PÉREZ LUÑO A. E., Libertad informática y leyes de protección de datos personales, Madrid, Centro de Estudios Constitucionales, 1990.–

MARTÍN, M. W., SCHINZINGER, R., Ethics in Engineering, New York, McGraw Hill, 1989.–

MATURANA, H. R., VARELA, F. G., El árbol del conocimiento, Santiago de Chile, *Editorial Universitaria*, 1988.–

MASUDA, Y., La sociedad informatizada como sociedad postindustrial, Madrid, Fundesco/Tecnos, 1984.–

MURILLO, P. L., El derecho a la autodeterminación informativa, Madrid, *Tecnos,* 1990.–

NORA, S., MINC, A., La informatización de la sociedad, México, Fondo de Cultura Económica, 1980.–

WINOGRAD, T., FLORES, F., Understanding Computers and Cognition. A new Foundation for Design, Reading, Addison Wesley, 1986.

Y hasta aquí la propuesta, ahora habría que ponerla en práctica por medio de la realización de las acciones más adecuadas. El mejor consejo para estas acciones es el de que se desarrollen con prudencia, respetando el contexto en el que se desenvuelvan los interesados en su puesta en práctica.

Aplicaciones informáticas en la enseñanza del derecho: reflexiones y métodos de calificación automática

RAFAEL GONZÁLEZ-TABLAS Y SASTRE

Profesor Titular de Filosofía del Derecho y de Derecho de la Informática de la Universidad de Sevilla

(ESPAÑA)

La Universidad española, como cualquier otra institución, no existe en un vacío social sino en un mundo real lleno de dinamismo. Este aspecto ha sido señalado en el informe elaborado por los miembros de la misión del International Council for Educational Development (ICED): «Durante las dos últimas décadas el entorno socioeconómico y político de las Universidades españolas ha experimentado cambios extraordinarios de los tipos más diversos, y probablemente todavía puedan producirse otros de grandes dimensiones. Por tanto, y si desean elevar al máximo su aportación al progreso de la nación, el reto o desafío fundamental con el que se enfrentan las Universidades españolas es el de hacer frente y mantenerse a la altura de esos cambios básicos que se están produciendo a su alrededor.»[1]. Además, en su informe la Secretaría General, destaca junto a los cambios políticos, económicos, sociales y culturales, los grandes cambios demográficos de las últimas décadas que, «han tenido, y continuarán teniendo, importantes repercusiones sobre el sistema educativo español, así como sobre las oportunidades de empleo de los jóvenes»[2]. Cuatro son los tipos de cambios demográficos experimentados

[1] A.A.V.V. La reforma universitaria española. Evaluación e informe. Internacional Council for Educational Development. Consejo de Universidades 1987, pp. 17.

[2] Ibídem. pp. 18.

por la sociedad española, de los que sólo nos vamos a referir al primero, en el que se destaca la alta tasa de natalidad conseguida en España hasta 1964, alcanzándose su máximo y situándose en el 21 por mil de la población. Durante la década siguiente, entre 1965 y 1976, se produce un lento descenso de la misma, para ir acelerándose rápidamente hasta situarse en una tasa del 13 por mil en 1985. Aunque este descenso ya se ha dejado sentir en la escuela primaria las matriculaciones «siguen aumentando en la educación superior, en la que el impacto del descenso demográfico no se dejará sentir hasta finales de la década de los 90. E incluso entonces puede verse al menos parcialmente contrarrestado por una mayor participación en la educación universitaria por parte de los adultos y de los jóvenes del medio rural»[3]. Y por último, el cambio sociológico –especialmente significativo– y que se refiere al «reciente y espectacular aumento del número de mujeres matriculadas en la Universidad, que pasó del 37% del total en 1975-76 en las diversas facultades, escuelas universitarias y centros técnicos, hasta aproximarse en el momento actual a condiciones de igualdad con los varones.»[4].

Todos estos cambios demográficos, económicos, políticos, sociológicos, etc. han tenido y tienen una especial incidencia en la Universidad, pero entre todos ellos, el que se ha destacado con más fuerza es el demográfico, que hizo que el número de los alumnos matriculados en las universidades se duplicara en la década de los 60, para casi volverlo a hacer durante la de los 70 y aumentar en más de un tercio en la de los 80. La tendencia es a que siga creciendo no esperándose una reducción suficientemente significativa hasta finales de la década de los 90. Como dato meramente indicativo: en el curso 1988-89, en la Facultad de Derecho de Sevilla, hay seis Grupos en el Primer Curso. Pues bien, en el Grupo «A» (no es el más numeroso) la capacidad del aula es de 156 puestos fijos al que asisten 310 alumnos. Otro dato indicativo es que del total de alumnos asistentes las mujeres representan ya el 58,3871% (181 alumnas), mientras que los hombres son el 41,6129% (129 alumnos).

Esta realidad plantea un reto de futuro al que no podemos ser ajenos los profesores universitarios. La Universidad, difícilmente podrá cumplir con el servicio público de la educación superior, así como sus funciones de creación, desarrollo, transmisión y crítica de la ciencia, la técnica y la cultura, o, atender a la preparación para el ejercicio de actividades profesionales, etc.; si no se tiene en cuenta este difícil problema de la masificación. Así pues, este crecimiento de la demanda de educación superior implica la existencia de

---

[3] Ibídem. pp. 18.

[4] Ibídem. pp. 19 y ss. (...), conviene señalar que las mujeres matriculadas siguen concentrándose fundamentalmente en áreas educativas consideradas tradicionalmente como «femeninas», tales como magisterio, enfermería y humanidades, lo que indica que los bastiones masculinos tradicionales no han sido todavía conquistados (...), resulta especialmente significativo que el porcentaje de mujeres matriculadas en las enseñanzas técnicas haya pasado de sólo el 3,4% en 1975-76, al 12,2% en 1983-84, habiendo continuado ascendiendo desde entonces.

gravísimos desequilibrios, y entre ellos, el que resulta particularmente afectado es el de la calidad[5]. Para los miembros de la misión del ICED hay que cambiar los criterios con que se juzgaba la calidad de un centro universitario, consistentes en evaluar «la cantidad y calidad de sus «inputs» en relación con el número de alumnos, en lugar de por su «outputs» (...). La prueba de fuego de la calidad de una Universidad consiste en la diferencia entre lo que sus alumnos, tanto graduados como no graduados, llevaron inicialmente a la misma y lo que extraen de la institución, en términos de conocimientos, habilidades intelectuales, capacidades analíticas, valores, actitudes y motivaciones (...), la prueba última y definitiva es la de qué hacer luego con todo lo que han aprendido, hasta qué punto resulta pertinente y útil para su vida futura, para su familia y su comunidad, así como para la sociedad en general.»[6]. Por otro lado, el Consejo de Universidades señala entre los objetivos de la reforma de las enseñanzas universitarias: «1.º Actualizar las enseñanzas y conocimientos que se imparten en las Universidades españolas incorporando otras nuevas que el desarrollo cultural, científico y técnico exige, facilitando la formación interdisciplinar e incluyendo en los currícula universitarios enseñanzas instrumentales (como lenguas modernas o informática) que deben incluir hoy parte del bagaje intelectual de todo universitario.» Este somero análisis de la realidad universitaria conduce directamente a la siguiente conclusión: una buena forma de plantear el reto de la enseñanza y la investigación en la universidad actual, para aumentar su calidad, es la de plantearse un proyecto de investigación, que pueda dotar al profesor universitario de un soporte tecnológico adecuado para una exigente y rápida calificación de los alumnos.

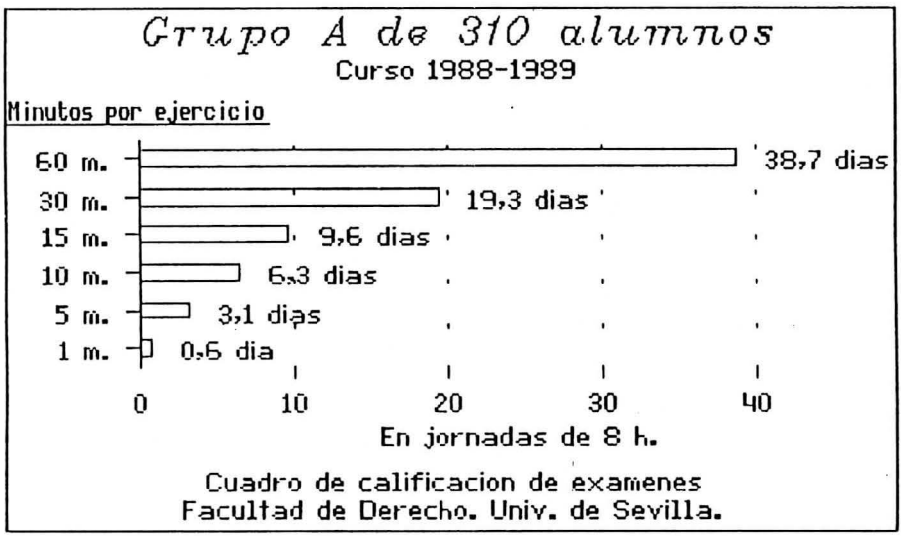
En efecto, tomando como base los datos del Grupo «A», tenemos que para el presente curso académico (de octubre a mayo), en nuestra disciplina, se impartirán 90 horas lectivas. Pues bien, para calificar un examen parcial, por ejemplo escrito, correspondiente a las 30 horas de explicaciones del primer trimestre, el profesor, en función del tiempo que se requiera dedicar a cada ejercicio, puede tardar en hacerlo los tiempos expresados en el siguiente cuadro, expresado en jornadas de ocho horas, que pone en seguida de mani-

---

[5] Ibídem. pp. 65 y ss. Pero, hoy por hoy, tampoco resulta un argumento absoluto si atendemos a la experiencia de numerosos países, incluido el nuestro. Dos datos se apuntan como compensadores de esta pérdida en la calidad de la enseñanza. El primero procede de la cantidad misma de alumnos, que al aumentar considerablemente su número, diversificó su procedencia, concediendo más oportunidades a algunos muy capaces y motivados, tanto profesional como académicamente. Se ha demostrado que el rendimiento medio del nuevo estudiantado no resulta inferior al del antiguo sistema más selectivo y rigurosamente elitista. El aumento de alumnos más capacitados y motivados ha compensado el descenso en la calidad desde el punto de vista del rendimiento social. El segundo dato procede de la renovación y adaptación de la oferta educativa a un tipo de alumnado más diversificado, intentando incorporar, con un ritmo acelerado, la explosión de nuevos conocimientos y los cambios revolucionarios que la tecnología está produciendo en todas partes.

[6] Ibídem. pp. 68-69.

fiesto las dificultades que se tienen para poder examinar adecuadamente a un alumno. Así dedicar un tiempo cercano a una hora de calificación por cada alumno es del todo imposible. Y, por ello, lo que se puede comprobar, qué sabe el alumno de la materia explicada, es una mínima parte. De ahí, que los profesores no tengamos ya la seguridad de que nuestros alumnos saben y comprenden todo lo que hay que saber y comprender de la disciplina. Es pues, urgente, investigar en las aplicaciones instrumentales de la informática, para conseguir elaborar programas de ordenador capaces de ser aplicados a la enseñanza en torno a estos tres objetivos fundamentales: 1) La calificación automática. 2) La simulación por ordenador. 3) La enseñanza programada. Con la calificación automática se conseguirían una serie de ventajas que redundarían en una mejora de la calidad de la enseñanza.



En efecto, la labor de calificar es una de las más importantes que cumple el profesor, por la responsabilidad que conlleva. Pero, por sí misma, es una tarea pesada y aburrida, que no gratifica al profesor. Tampoco es de gran utilidad para el alumno ya que son pocos los verdaderamente interesados en que se le indiquen sus errores, o los que solicitan consejos para enmendarlos. La calificación ha dejado de ser una parte de la enseñanza para convertirse en el dato burocrático que indica el final del estudio de una determinada disciplina. El profesor ya no es, por desgracia, el «Maestro» que ayuda y encauza los esfuerzos de sus alumnos para superar los difíciles obstáculos que el rigor de los estudios impone. El profesor calificador es, de hecho, el principal enemigo del alumno. Con la calificación automática por ordenador,

la calificación recuperaría su ser dentro de la enseñanza. El profesor sólo tendría que fijar los criterios y parámetros, que desde su responsabilidad, considera que son necesarios para obtener una calificación suficiente. Fijados éstos en el programa, no olvidemos que quien verdaderamente califica es el ordenador, el ordenador liberará al profesor de la dedicación aburrida y poco gratificante de calificar. Y lo hará, manteniendo siempre el mismo nivel de atención y objetividad frente a los alumnos, sin que estos puedan influirlo, cansarlo o distraerlo. El ordenador calificador se convierte así en el enemigo del alumno, y el profesor puede ser, de nuevo, el «Maestro» y aliado de sus alumnos que enseña y ayuda cómo superar las dificultades que pone la máquina. El profesor puede dedicar más tiempo a enseñar y a investigar. Pero no es ésta la única ventaja de la calificación automática. Sólo, por citar alguna otra, que redunda directamente en la calidad de la enseñanza, diré que los alumnos aventajados no se ven lastrados por los más torpes o desinteresados. Cada alumno podría marcarse su propio ritmo de estudio personalizándose aun más la enseñanza. Los otros dos objetivos, la simulación y la enseñanza programada, se iniciarían una vez logrado este primero, que rentabilizaría más rápidamente la investigación efectuada.

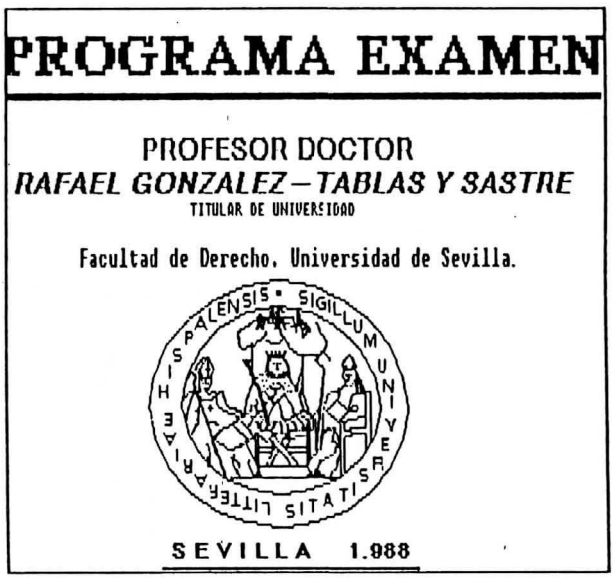


Figura 1

En esta línea de investigación he desarrollado un primer programa de exámenes que funciona desde el curso 1988-1989 y que hasta la fecha ha rendido a plena satisfacción. El alumno se enfrenta directamente con el ordenador cuando considera que su preparación de las pruebas es la suficiente. Así, cuando se ha terminado de explicar la materia correspondiente a una de las pruebas de ordenador los alumnos pueden desde ese momento examinarse con los mismos. Para una mayor facilidad se les permite hacer un segundo intento por cada una de las pruebas en el supuesto de que se hubiera suspendido la primera. Para la calificación final solo se toma la mejor de las dos notas.

La primera pantalla que se encuentra el alumno cuando se examina es la que se reproduce en la figura 1. Al pulsar cualquier tecla aparece un menú en el que se le solicita que pulse el número correspondiente al libro o artículo objeto de la prueba, de una lista que se ofrece en la pantalla. Seleccionado éste, se pasa a otro menú que solicita el Capítulo o el Parcial correspondiente[7]. De aquí, se pasa a una tercera pantalla que solicita los datos personales del alumno, tales como sus apellidos y nombre, y el grupo al que pertenece. A continuación el ordenador comprueba la veracidad de estos datos, así como las pruebas que ha realizado el alumno, informándole del resultado de las mismas, por ejemplo: «*Te examinaste por 1ª vez el 15-12-1991 del 1º Parcial y sacaste un NOTABLE 8*». Una vez informado de los datos, el ordenador presenta una pantalla en la que advierte que en unos instantes comenzará el examen para que el alumno se prepare.

El examen consiste en cincuenta preguntas que el ordenador selecciona de una forma aleatoria de un fondo que puede ser tan amplio como se quiera[8], generando la secuencia de las cincuenta preguntas a partir de una semilla que toma de su propio reloj cuando el alumno ha terminado de introducir sus datos. De este modo, la variedad de exámenes que con el mismo fondo de preguntas se puede generar es enorme, y es muy difícil que se den dos exámenes iguales. Cada pregunta dispone de un tiempo de respuesta que está en función de la longitud del la misma, es decir, en función del número de caracteres que la componen.

---

[7] Todos los gráficos de resultados que se ofrecen se refieren a los Capítulos 3, 4, 5 y 6 del libro del Profesor Antonio-Enrique Pérez Luño «Derechos Humanos, Estado de Derecho y Constitución». Cuarta edición aumentada. Madrid. Editorial Tecnos, 1992.

[8] Los fondos están normalmente constituidos por unas doscientas preguntas.

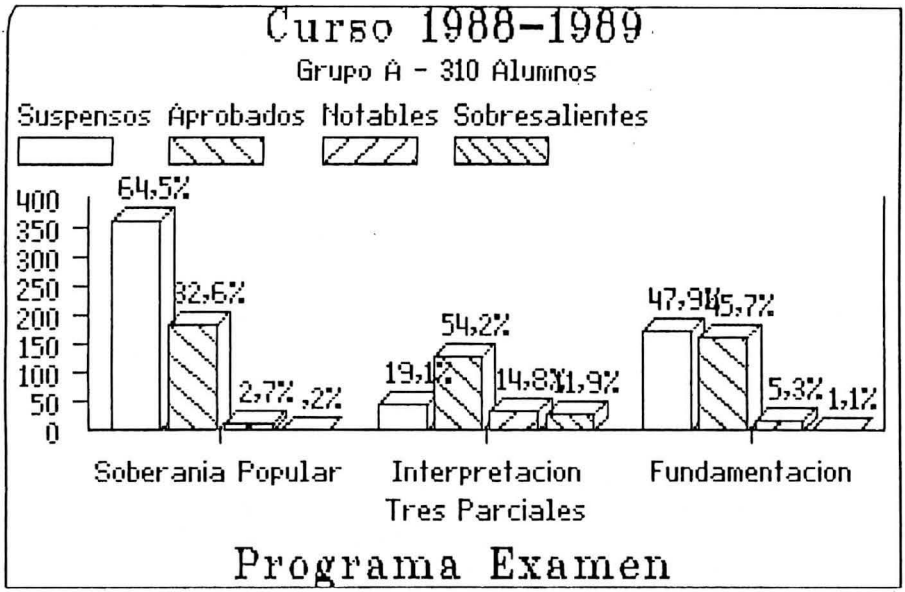


Figura 2

Si bien, en la pantalla aparece un contador que empieza en 60 y va decreciendo hasta llegar a cero, haciéndolo más deprisa o más despacio según sea el tiempo calculado para cada pregunta. El calculo del tiempo de cada pregunta se ha hecho para una velocidad de lectura que resulta necesaria es la de unas 70 a 75 palabras por minuto que constituye una velocidad muy lenta. Las preguntas sólo pueden ser Verdaderas o Falsas y en consecuencia solo hay que pulsar la letra «V» cuando la pregunta es Verdadera y la letra «F» cuando la pregunta es Falsa. Así pues, el alumno tiene que reconocer mediante una lectura comprensiva los párrafos del libro que constituye la materia de examen sabiendo que son verdaderos los que se ajustan exactamente al texto, en tanto que resultan falsos aquellos que de algún modo se apartan del mismo. La tabla de verdad es el texto propuesto, es decir, que en las preguntas verdaderas no se pretenden que lo sean de un modo absoluto e incondicionado, sino que lo son en función del texto que constituye su tabla de verdad. De este modo, se produce una certeza absoluta sobre cuáles son las preguntas verdaderas y cuáles son las falsas, exigiéndose siempre el conocimiento del texto propuesto. Además, existe el mismo número de preguntas verdaderas como de falsas con lo que se elimina,

en parte, la posibilidad de aprobar contestando siempre verdadero en el supuesto de que el fondo contuviese un número mayor de preguntas verdaderas que de falsas, lo contrario, también es cierto.

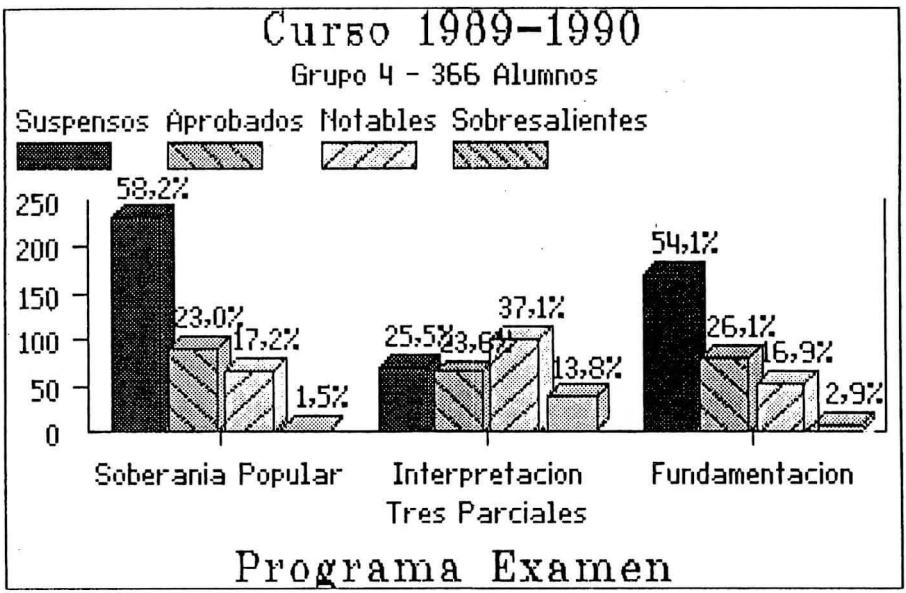


Figura 3

Cada vez que el alumno contesta incorrectamente a una de las preguntas el ordenador le informa de esa circunstancia mediante el siguiente mensaje: «Su respuesta es incorrecta», al tiempo el ordenador actualiza el contador de errores (que siempre aparece en la pantalla) añadiendo uno al mismo. Cuando el ordenador comprueba que se han cometido 11 errores corta la secuencia de preguntas y pone la calificación de Sobresaliente, Notable, etc. con la numérica correspondiente. La calificación se calcula para los aprobados restándole medio punto por error y para los suspensos por tramos de proximidad a la pregunta cincuenta[9].

Los resultados globales de la aplicación son los que se muestran en las Figuras 2, 3 y 4 que se corresponden con los Cursos 1988-1989, 1989-1990

[9] Así once errores en la pregunta cincuenta equivale a una nota de SUSPENSO 4,5.

y 1990-1991, los correspondientes al curso 1991-1992 es similar a los anteriores. De la observación de los mismos se comprueba que el primer parcial correspondiente al rótulo «Soberanía Popular» es el que acumula un mayor porcentaje de suspensos, ello es lógico por dos razones: la primera por ser la primera vez que se examinan con este sistema; y la segunda, last bus not least, por ser el primer examen de una materia que inicialmente les resulta totalmente desconocida, incluso en sus términos más comunes. El segundo parcial, «Interpretación», está deliberadamente reducido en su materia y así resulta comparativamente más fácil que los otros dos. Ello sirve para animar a los que han fracasado en el primero por una especial inadaptación al sistema y evitar así el abandono prematuro del estudio de la asignatura por parte de esos alumnos. En cuanto al tercer parcial «Fundamentación» es conceptualmente más difícil y exige un estudio más reposado, pero ya no se tienen los inconvenientes del primer parcial, es decir, ya se conoce el sistema y también se conoce la terminología de esta asignatura, así como, el vocabulario del resto de las disciplinas que componen el primer curso.

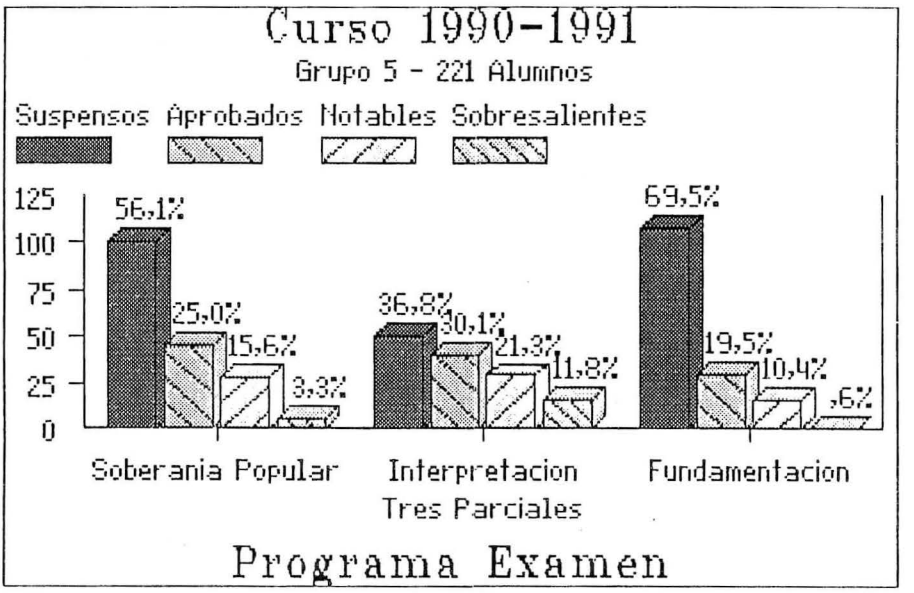


Figura 4

El programa, fue inicialmente diseñado para medir el grado de comprensión de un texto determinado y, exige un verdadero conocimiento del mismo,

jugando verdaderas malas pasadas a los que hacen primar la memoria sobre la compresión del texto. Se ha demostrado que se adaptan más rápidamente al sistema de examen los alumnos que no intentan competir en memoria con el ordenador, y aquellos alumnos que hacen un uso abusivo de la memoria tienen grandes dificultades para conseguir los resultados a los que su espléndida memoria les tiene acostumbrados.

Situación del derecho informático en España y en Europa: algunas consideraciones

VICENTE LÓPEZ-IBOR MAYOR

Jefe del Departamento de Relaciones Internacionales de UNESA
Asesor técnico de su Comité de Relaciones Internacionales
Director del Proyecto SEDE
Presidente del Grupo de Informática Jurídica de UNESA

SONSOLES GARCÍA DELGADO

Analista Jurídico del Proyecto SEDE
Miembro del la Asesoría Jurídica y del Grupo de Informática Jurídica de UNESA

(ESPAÑA)

I. INTRODUCCION

Cualquier análisis detenido y riguroso de la sociedad contemporánea nos debe conducir a reconocer que hoy ya las tecnologías de la información y de la comunicación, es decir, el conjunto formado por la informática, la electrónica, y las telecomunicaciones componen el «sistema nervioso» de nuestras sociedades. El Profesor Julián Marías, en uno de sus valiosos ensayos, ha escrito que «la electrónica es con la energía nuclear el factor técnico más importante en la transformación del mundo y de las condiciones de vida humana en el siglo XX», añadiendo que «la energía nuclear como la electró-

nica representan el paso a un orden de una magnitud superior dentro de las técnicas científicas».

El conocimiento –o información ordenada– constituye la piedra angular del cambio en esta nueva sociedad en que la informática y las telecomunicaciones aportan nuevos medios para capturar, almacenar, desarrollar, transmitir y difundir información.[1]

En un interesante análisis sobre el advenimiento de las nuevas tecnologías de la información realizado hace una década se decía que en los próximos años asistiremos sin duda a la comercialización a escaso precio de equipos para traducción en lenguaje natural de sistemas para la seguridad del domicilio, se podrán realizar todo tipo de operaciones de telecompra, telebanco, un médico podrá ser consultado por teléfono, con envío inmediato de receta, un cultivador agrícola se informará de las cotizaciones, tratará con el comprador, mayorista, supermercado o detallista, que a su vez estará enlazado por su terminal a bolsas electrónicas de cada producto: legumbres, cereales, carne, etc. La terminal, una vez concluida la transacción imprimirá los albaranes y las facturas y retendrá lo escrito. Estas comunicaciones personales serán completadas por un sistema de comunicación colectiva: el conjunto de la red telefónica transmitirá, al mismo tiempo que la voz, mensajes de todas clases. La mayor parte de las empresas enlazarán entre ellas con aparatos de trabajo administrativo.

Se dictará un texto a una máquina de escribir que, reconociendo las palabras, las imprimirá. Los satélites entrarán vertiginosamente en escena. Mañana el corazón y los demás órganos funcionarán bajo un sistema de información de autovigilancia: más aún el detector de anomalías disparará automáticamente la acción correctora[2]. Podemos afirmar que buena parte de estas previsiones ya han sido cumplidas. En efecto, hoy las nuevas tecnologías de la información están próximas a alcanzar su mayoría de edad. Como ha señalado Alvin Toffler[3] , los lectores ópticos, los dispositivos de rayos láser, los ordenadores de mano y otras tecnologías de vanguardia están inundando farmacias, grandes almacenes, comercios de descuento, librerías, almacenes de materiales y aparatos eléctricos, fruterías, comercios de confección, tiendas especializadas y boutiques de todo tipo. En un mundo donde el dinero está «informatizado» y la información «monetarizada» el consumidor paga dos veces cada compra que hace: la primera en metálico y la segunda con una aportación de información que vale dinero. La información se ha convertido, por consiguiente, en la gran protagonista y palanca o núcleo de poder de nuestro tiempo. La Información con su poliédrica presentación, y las tecnologías en que se apoya. Así lo han subrayado M. Mirabito y Barbara L.

---

(1) FERNANDO BONDIA. «Propiedad Intelectual (su significado en la sociedad de la información)». *Editorial Trivium*. 1988, pág. 17.

(2) FRANÇOIS MITTERAND. Aquí y Ahora. *Argos Vergara*, 1981.

(3) ALWIN TOFFLER, El Cambio del poder. Powershift. *Plaza y Janes*. 1990 pag. 129 y ss.

Morgenstern, «Information does not simply consist of television programs, computer data, telephone conversations, and music stored on records. Information is also a picture manipulated by a computer that highlights the details of the human body that were hitherto invisible. Information is a library of that have been coded and stored on a handful of optical recording discs. Information is a series of facts and figures that depict the current state of the stock market. This information can then be accessed at home via a personal computer. These are only a few examples of the various types and forms of information.

It is also important to note that information can be viewed as a commodity. In the traditional communications industry, television and radio programs are assigned a financial value that varies in accordance with a given show's ratings. The information generated by non-traditional tools can be similary valuable».[4]

Por consiguiente, procede constatar que nuestro planeta se encuentra surcado por un espeso entramado de redes intercontinentales de transferencia de información científica y tecnológica, que permiten vía terminal conectada –por teléfono– a un host o a bases de datos concretas o mediante el uso de información almacenada en CD-ROM –en discos ópticos– acudir a recursos de información extremadamente valiosos. Las más de 3.900 bases de datos existentes actualmente en el mundo –en diferentes tipos de soportes– cubren virtualmente cualquier tipo del saber, registrándose millones de referencias relativas a artículos de revistas, informes técnicos, patentes, manuales, conferencias, catálogos, tesis, documentos gubernamentales, etc. Además docenas de bases de datos numéricas ofrecen series económicas y financieras, resultados de empresas, legislación, doctrina jurídica y jurisprudencia, bolsas de trabajo, plazas hoteleras. Unos pocos minutos de trabajo en un terminal bastan para localizar virtualmente cualquier información o su fuente, pública o inédita. Hoy puede pensarse en informaciones que atraviesan la sociedad y que circulan entre las personas gracias a la difusión capilar que provoca la informática distribuida.[5]

II. LA CONSTRUCCION DEL DERECHO DE LAS TECNOLOGIAS DE LA INFORMACION

No cabe, por tanto, sorpresa alguna que estos fenómenos de tan profunda y extensa incidencia social reclamen una atención cada vez más acusada por parte del Derecho, ya que, al ser la sociedad el medio específico en el que

[4] The new communications technologies. MICHAEL M. MIRABITO. BARBARA L. MORGENSTERN. *Focal Press*. Boston, London, 1990, pags. 4 y ss.

[5] Ver: FEDERICO MAYOR ZARAGOZA. «Mañana siempre es tarde». *Editorial Espasa Calpe* 1990. Ver también V. LÓPEZ-IBOR MAYOR «La sociedad de la información» Conferencia pronunciada en Abril de 1992. Fundación Tomás Moro. Madrid.

se produce el Derecho, a éste le corresponde dar permanente respuesta a los nuevos desafíos que de la misma emergen.

Es ya clásica la distinción al afrontar la relación Informática-Derecho, entre la Informática Jurídica y el Derecho de la Informática. Aquélla nos descubre, cada vez con mayor versatilidad, los útiles que las nuevas tecnologías son capaces de poner al servicio del mundo del Derecho. Y también nos ofrece el panorama de las nuevas destrezas que los juristas han adquirido no sólo en el conocimiento y empleo de la técnica informática sino, lo que es mucho más importante, en el avance hacia la mejor conexión entre el conocimiento jurídico y su presentación o representación a través de procedimientos y medios informáticos. Con la expresión de Derecho de la Informática, o empleando la expresión que nosotros juzgamos más certera, «el Derecho de las Tecnologías de la Información», se trata de delimitar una disciplina emergente que cuenta ya sin embargo, a nuestro juicio, con solidez bastante en el cuadro actual de las Ciencias Jurídicas.

La formación o mejor la configuración, es decir, el hecho de reconocer el encaje de una nueva disciplina no es tarea sencilla ni mucho menos pacífica. Tarea que incorpora como primer cometido el de reconocer un camino que nos permita «identificar» sus límites propios que justificarán o negarán la inclusión de la nueva disciplina, y su admisión como tal en el ámbito de las Ciencias Jurídicas. Especialmente atinada y extrapolable a nuestro caso me parece la reflexión de Aguilar Navarro con relación a la definición del Derecho Internacional Público. Señala que ésta es empresa arriesgada no sólo por cuanto toda definición constituye una concesión dogmática y apriorística, sino por lo prematuro que puede ser el intento cuando aún carecemos de la perspectiva histórica, que es la que nos puede trazar la línea esencial y existencial de nuestra disciplina. Lo que parece acaso más recomendable es proceder a una somera descripción de la realidad (fáctica y normativa) sobre la que opera el Derecho (Internacional Privado), para después situarle en relación con otras ramas jurídicas que tienen afinidades y semejanzas nacidas de los hechos e impuestas por la peculiaridad de sus normas y de **sus mecanismos** técnicos.

El problema, por tanto, de la autonomía del Derecho Informático o, del Derecho de las tecnologías de la información, debe ser contemplado con serenidad crítica. Ha escrito Berliri –con relación al Derecho Financiero– que el problema de delimitar una nueva disciplina como autónoma de las otras, es también un problema de oportunidad de desgajar una serie de normas que se refieren a una serie de relaciones para poner de manifiesto afinidades y divergencias y construir un sistema armónico que permita una cooperación, integración e interpretación de las normas que transcienda al mensaje literal.

Ciertos ámbitos de la realidad social exigen una normación jurídica sustancialmente diversa a la de otros. La singularidad de cada uno de estos grupos de normas explica la aparición de distintas disciplinas jurídicas.

El hecho de que la construcción del Derecho Informático tenga una limitada extensión en el tiempo y en el espacio o que carezca por ello de una escasa o breve ordenación historiográfica queda, a nuestro juicio, plenamente superada y resuelta por la velocidad y prodigalidad de los acontecimientos que han ido trazando en la última década las trayectorias de su plural ordenamiento. Ordenamiento que se armoniza sin embargo en el rumbo común de un Derecho propio, cuyas notas pasamos a definir.

Nos encontramos pues ante un Derecho nuevo, con un grado incipiente de desarrollo y, por tanto, estamos en presencia de un marco jurídico en vías de formación. Ello implica que las relaciones jurídicas que en el mismo se producen no puedan adaptarse fácilmente a normas rígidas de encuadramiento y que se manifiestan por ello rebeldes a las viejas clasificaciones. El Derecho informático se caracteriza por su naturaleza multidisciplinar y su reglamentación tiende a cubrir, en esencia, gran número de aspectos que inciden, directa o indirectamente, en casi todas las disciplinas jurídicas: Constitucional (protección de los datos personales; reconocimiento de la libertad informática; los procedimientos de formación de las Leyes); Civil y Mercantil (establecimiento de nuevas fórmulas contractuales. Responsabilidad civil en la gestión de las bases de datos o por funcionamiento inadecuado del programa; propiedad intelectual –protección jurídica de los programas de ordenador); Penal (protección jurídica del Software. Delito informático); Procesal (Documento informático y valor probatorio); Bancario; Laboral; Comunitario; etc.

Otra nota característica del mismo viene dada por su implicación o interpenetración con un lenguaje –el informático– acusadamente técnico, que empieza a constituir, en algunos casos, un auténtico desafío para la labor interpretativa del jurista.

Asimismo, este nuevo Derecho tiene un indiscutible carácter internacional y transnacional. Se trata de un Derecho fundamentalmente establecido a impulso de los foros internacionales y con referencia expresa a los problemas que en ese ámbito se han ido detectando.

El Derecho Informático se nos presenta, pues, como un Derecho nuevo, es decir, en continua formación y evolución, multidisciplinar, con amplio radio material y geográfico de influencia, flexible –de acuerdo con la naturaleza de la actividad y buena parte de las relaciones que está destinado a normar– y con una clara vocación reformadora, es decir, no acomodaticio a los moldes tradicionales del Derecho[6].

Una buena parte de la mejor doctrina española se ha manifestado inequívocamente a favor de este nuevo Derecho. Así, el Profesor Pérez Luño ha

[6] VICENTE LÓPEZ-IBOR MAYOR «La legislación sobre informática en el ordenamiento jurídico español. Congreso sobre Derecho Informático, Zaragoza. Facultad de Derecho, 22-24 de junio 1989, pags. 417 y ss.

manifestado con claridad que nos hallamos ante la aparición de una nueva disciplina jurídica y no de un mero rótulo para reagrupar una serie de problemas conexos con un campo de estudio peculiar. El Derecho de la informática posee idénticos títulos científicos para constituirse en disciplina autónoma como antes los tuvieron otras materias jurídicas novedosas como, por ejemplo, el derecho aeronáutico, el derecho espacial, el derecho comunitario... (cabría recordar muchas otras disciplinas que coinciden, en esa aspiración o título de disciplina autónoma; el nuclear, el eléctrico, el agrario, el derecho de los consumidores, del consumo)[7]. Pueden, según Pérez Luño, aducirse, entre otras, las razones siguientes en favor de la sustantividad y autonomía científica del Derecho de la informática.

1) Existencia de un objeto delimitado constituido por la propia tecnología de las computadoras, cuyas implicaciones económicas, sociales, culturales y políticas son tan profundas como evidentes hasta el punto de que el Derecho no puede desentenderse de su reglamentación. Una tecnología como la informática, que parece abocada a incidir en casi todos los aspectos de la actividad humana, forzosamente tenía que hallar su correlato normativo, pues el Derecho supone precisamente la principal técnica de organización de la vida social. **En efecto el carácter «horizontal» o transversal de esta disciplina parece claro aunque no imposibilita en absoluto el que las relaciones que genere tengan puntual respuesta en un corpus completo y coherente de disposiciones capaz de responder adecuadamente a esta nueva problemática.**

Si la informática constituye el objeto inmediato del derecho de la informática, su objeto mediato es la propia información. Se ha indicado que la información constituye el bien inmaterial, el producto autónomo y previo a todo el procesamiento y transmisión que de ella pueda realizarse. La información se desglosa en dos momentos: el primero tendente a dar

---

[7] Se habla de Derecho Bancario, Minero o de Montes, o Sucesorio (Ver Diritto Forestale e vincoli idrogeologici. CESARE CANTELMO; Universitá degli Studi di Viterbo. 4.º Congreso Internacional sobre Informática y Reglamentación Jurídica. Roma 16-21, Mayo 1988).

Ver también: «Panorámica general de la protección jurídica de los programas de ordenador por el derecho de autor en Francia». Comunicación de LUIS MARÍA MIRANDA SERRANO, presentada en el Congreso sobre Derecho Informático celebrado en Zaragoza los días 22-24 de junio de 1989.

«Los nuevos avances tecnológicos operados en el terreno de la Informática, ha dado lugar a que se hable de una nueva parcelación jurídica acotada «in abstracto» por diversas relaciones posibles entre Derecho por un lado e Informática por otro. En este sentido no ha de extrañarnos, pues, que cada vez de forma más intensa se emplee la expresión «Derecho Informático».

Según el profesor GALINDO («Consecuencias de la entrada de España en la Comunidad Europea en el Derecho español de la informática» Secretariado de publicaciones de la Universidad de Zaragoza): Esta denominación es inapropiada, ya que hoy en día es preciso considerar no tan solo a los ordenadores y sus consecuencias, sino también a las tecnologías de la comunicación y la información.

Ver también: HUET JEROME. Du droit de l'informatique au droit des telécomunications-problématique générale. 1988.

forma y significado a un determinado mensaje; el segundo dirigido a su transmisión. Se trata de dos etapas de una función única que consiste en transmitir mensajes, conocimientos e ideas, es decir, la comunicación. **(Antes analizábamos, coincidiendo con este planteamiento, el proceso informativo y sus contenidos).**

2) Existencia de una metodología específica para abordar adecuadamente esta nueva disciplina jurídica. La comprensión correcta de los problemas planteados por las nuevas tecnologías de la información (informática) y de la comunicación (telemática) exige contar con unas categorías conceptuales y metódicas aptas para captar su alcance y significación.

3) Existencia de unas fuentes legislativas, jurisprudenciales y doctrinales del Derecho de la informática, que en los países más avanzados han conducido a la planificación de cursos universitarios regulares encaminados a organizar su enseñanza, así como la continua celebración de congresos, coloquios y seminarios dirigidos al estudio de estos materiales normativos, de los que constituye un excelente ejemplo el que ahora celebramos.

II. ALGUNAS PROPUESTAS COMUNITARIAS SOBRE EL DERECHO INFORMATICO

Es interesante constatar cómo más allá del panorama que nos ofrece la formación y sistematización del Derecho informático a través de las normas jurídicas –norma agendi– que producen los ordenamientos nacionales que, la propia Comunidad Europea viene desplegando también una labor de primera magnitud en la construcción, directa e indirecta de este Derecho. Construcción que tiene valor y significación sigulares ya que por su propia vocación, el Derecho Comunitario tiende, en no pocas de sus producciones normativas a realizar un equilibrio no solo material sino también formal entre tradiciones juridico-europeas bien diferentes.

En concreto en el campo de las tecnologías de la información se han detectado ya numerosísimas disposiciones que abarcan todos los ámbitos de interés de esta disciplina. En su propio derecho originario existen referencias claras a acciones en este ámbito (Política de telecomunicaciones, I+D, etc.). En este trabajo recogemos algunas de tales disposiciones, juzgadas especialmente relevantes o significativas, dictadas en los últimos años.

De acuerdo con la naturaleza del Derecho comunitario, el marco legislativo en esta materia se manifiesta en dos niveles diferentes:

- El Derecho originario previsto en los tratados constitutivos de la

Comunidad[8], así como aquellos textos que desde la constitución de la Comunidad han venido a completarlos y modificarlos[9].

– Normas jurídicas emanadas de las instituciones comunitarias[10] , en este sentido la Comisión ha propuesto un importante conjunto de medidas sobre los distintos ámbitos de protección relacionados con el uso de las nuevas tecnologías de la información.

1. Protección de la intimidad personal.

La necesidad de recoger o recabar, registrar y conservar información sobre la identidad de las personas o sobre circunstancias que conforman su vida y entorno personal no es algo nuevo que se haya originado con la informática. En cualquier caso, el impacto y efecto de aceleración que el deficiente uso político-social de la informática, puede provocar, al invadir la privacidad ajena o transgredir la frontera de los derechos fundamentales de la persona, merece una muy especial y seria atención y análisis. Se ha ejemplificado con agudeza este problema con relación al caso español, con motivo de las discusiones parlamentarias sobre la materia[11]: El ciudadano que ha depositado en los ordenadores de la Administración o de las empresas privadas (sus datos), se encuentra en la siguiente situación: Como contribuyente, Hacienda tiene no sólo su renta y su patrimonio, sino que además, a través del NIF, puede tener también todas sus operaciones contractuales, documentales, financieras, de valores, etc. Además estará registrando en los correspondientes registros mercantiles o de asociaciones su labor asociativa, su pertenencia a sociedades. Si ha cubierto, como hemos hecho todos, el censo de población y vivienda, el INE tiene además en su ordenador no solo la casa, descrita por

---

[8] El Tratado de Roma constituye la norma básica y documento clave que establece un marco coherente para la política de telecomunicaciones en la CEE. Considera a los organismos de telecomunicaciones de los Estados miembros como empresas comerciales, puesto que suministran bienes y servicios a cambio de un pago, estando pues sujetas al Derecho de competencia de la Comunidad, a las disposiciones sobre libre establecimiento y libre circulación de mercancías, y a las generales para aproximación de disposiciones legales reglamentarias y administrativas de los Estados miembros que incidan directamente el el establecimiento del Mercado Común.

[9] «El Acta Unica Europea vigente desde el 1 de julio de 1987, en el ámbito de las telecomunicaciones, ha supuesto un papel importante en la medida en que pretende favorecer el acceso de todos los Estados miembros a las nuevas tecnologías en igualdad de condiciones».

[10] Dentro del Derecho Derivado pueden establecerse distintos tipos de actos normativos:

– Actos típicos: aquellos que tienen su tipificación en los Tratados.

– Actos atípicos: aquellos que las instituciones adoptan sin ajustarse a ninguna de las categorías previstas en los Tratados.

– Actos vinculantes: actos jurídicamente obligatorios. A su vez éstos pueden tener efecto directo o por el contrario necesitan normas de transposición en los diferentes Estados miembros.

– Actos no vinculantes: actos que contienen acuerdos de principio, en materias en que los Estados miembros aún no están preparados para obligarse más en concreto, pero que pueden ser origen en el futuro, de la adopción de actos típicos vinculantes (reglamentos, directivas...).

[11] Ver Diario de Sesiones del Congreso de los Diputados, de 26 de junio de 1991. Intervención de D. FEDERICO TRILLO-FIGUEROA.

Ver también VICENTE LÓPEZ-IBOR MAYOR: «La sociedad de la información». Fundación Tomás Moro. (en especial el capítulo sobre «el peligro del ciudadano»).

ese ciudadano, sino además con quién vive y si lo hace de forma habitual o esporádica, su relación parental, su nivel de estudios, su grado de formación, su trabajo, su nivel dentro de ese trabajo, y hasta su cuarto de baño; si tiene calefacción y si esa calefacción es por gas o por sistema central. Pero, incluso, Hacienda podría tener en su ordenador que ese ciudadano ha querido contribuir con su impuesto a sostener una confesión religiosa oficialmente reconocida por el Estado. Es más, El Ministerio de Sanidad y Consumo de hecho tendrá qué enfermedades tiene o ha tenido ese ciudadano, cuáles son en Seguridad sus altas y sus bajas, cuáles sus médicos preferidos. Tráfico tendrá también si algún día ha conducido con irregularidad, en incluso si alguna noche se ha excedido al ingerir alcohol. Y si a ese ciudadano se le ocurre decir: voy a evadirme de este ambiente, ese ciudadano podría irse fuera de España pero, indudablemente, Iberia registraría su destino, la aduana registraría su salida, la empresa de viajes registraría su hotel y hasta en la factura del hotel los números de teléfono que marca, y la empresa de su tarjeta de crédito sin duda retendría hasta sus gastos mas reservados. ¿Se imaginan ustedes, que alguien pudiera disponer de todos esos datos al mismo tiempo sobre los ciudadanos españoles?.

«En nuestro tiempo, marcadamente informatizado y comprometido con los procesos de evolución tecnológica, el reconocimiento y la protección de los derechos individuales y de las libertades de información y comunicación se convierte en una tarea inexcusable de las sociedades democráticas. Por otra parte, la experiencia histórica pone de relive que la información al servicio del Estado con todos los medios de que éste dispone orientados a su obtención, revierte, cuando no se mide en la reducción del campo de la libertad, quedando ésta como un puro objeto de tolerancia observado por el poder. Del mismo modo, la labor de búsqueda de datos puede ser, en muchos momentos, perturbadora, no ya solo de actividades y conductas individuales, sino del propio cuerpo social en su conjunto».[12]

Con todo esto se perfilan dos riesgos muy definidos para el individuo:

a) La obtención de información sobre sus circunstancias o su conducta, sin su conocimiento y sin su consentimiento.

b) El uso ilícito de esa información, así como su cesión o transferencia ilícita.

Para hacer frente a estos riesgos se arbitró en un primer momento una solución viable[13]:

1. Solución técnica: Establecimiento de dispositivos físicos y lógicos de salvaguardia de la integridad de la información.

---

[12] VICENTE LÓPEZ-IBOR MAYOR. Congreso sobre Derecho Informático. Zaragoza junio 1989.

[13] Ver MANUEL HEREDERO «La protección de los datos personales registrados en soportes informáticos». Actualidad Informática Aranzadi. Enero 1992.

2. Solución deontológica: Reconocer a las personas titulares de datos, unos derechos sobre los mismos.

3. Solución jurídica: Desde este punto de vista, ya en el Consejo de Europa hacía referencia a la intimidad personal, este convenio surgió por considerarse insuficiente en art. 8.1 del Convenio Europeo de los Derechos Humanos, para proteger los datos personales registrados en soporte informático.

La Comisión, cree, sin embargo, que la situación actual de la Comunidad en lo relativo a esta cuestión resulta insatisfactoria. Cinco de los Estados miembros todavía no cuentan con una normativa jurídica en materia de protección de los datos, y los siete que cuentan con ella han elegido enfoques muy diversos, que van de lo liberal a lo restrictivo. El Convenio del Consejo de Europa deja abiertas muchas opciones y, además, sólo ha sido ratificado por siete Estados miembros. En consecuencia, la Comisión considera que debería existir un enfoque común de la protección de los datos a escala comunitaria. A juicio de la Comisión, ello contribuiría a asegurar el derecho fundamental a la intimidad de todos los ciudadanos de la Comunidad y a eliminar las actuales diferencias de trato que causan distorsiones de la competencia entre países comunitarios y obstaculizan el avance hacia el mercado interior. En este sentido se ha elaborado una iniciativa legislativa en la materia a través de tres propuestas comunitarias, excelente ejercicio teórico que nos muestra de nuevo la homogeneidad material del Derecho de las Tecnologías de la Información:

– Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales[14].

Con ella se pretende garantizar un alto nivel de protección, respetando el alcanzado por los Estados miembros que disponen de legislación nacional al respecto. Al mismo tiempo trata de introducir el nivel de protección mínimo del Convenio del Consejo de Europa para aquellos Estados que todavía no lo han ratificado.

Esta Directiva será aplicable tanto a los ficheros del sector público como del privado, comprendiendo por tanto los de la Hacienda Publica, salvo los relativos a servicios secretos y seguridad.

Establece un nivel de protección basado en la comunicación a la existencia de cualquier fichero, obligación de dar acceso a la información de cada ciudadano a su iniciativa con ciertas excepciones, entre las que se mencionan algunas relativas a la actividad financiera del Estado, y la obligación de rectificar los datos erróneos.

– Propuesta de Directiva del Consejo relativa a la protección de los datos personales y de la intimidad en relación con las redes públicas digitales de telecomunicación.

---

[14] COM(90) 314 FINAL – SYN 288. DOCE C 277, 5-11-1990.

Trata de satisfacer requisitos específicos con respecto a la protección de los datos personales y la intimidad convirtiéndolo en una condición previa esencial para lograr la aceptación pública de las nuevas redes y servicios digitales. En este sentido, la recogida, almacenamiento y tratamiento de los datos personales, sólo se justifica para proporcionar el servicio de que se trate, y no puede utilizarse sin autorización legal expresa o sin consentimiento previo del abonado para otra finalidad. Asimismo se limitan los datos personales a los datos de facturación en la medida que sean necesarios.

La utilización por el organismo de telecomunicaciones, de nuevas técnicas basadas en los requisitos de protección de los datos no podrán obstaculizar la libre circulación y comercialización de equipos y servicios de telecomunicaciones.

– Propuesta de Decisión del Consejo en el ámbito de la seguridad de información[15].

El Consejo en esta propuesta de Decisión adopta un plan de acción en el ámbito de la seguridad de los sistemas de la información (INFOSEC). El objetivo de dicho plan es desarrollar una estrategia global tendente a dotar a los usuarios de la información almacenada, tratada o transmitida por medios electrónicos, una protección de los sistemas de información frente a amenazas accidentales o deliberadas. Dicha acción tendrá en cuenta las actividades de normalización que se lleven a cabo en Europa y en el mundo.

2. Protección del trabajador.

En relación con la utilización de la informática como instrumento de trabajo, el art. 118 A del Tratado constitutivo de la Comunidad establece que los Estados miembros procurarán promover la mejora del medio de trabajo para proteger la seguridad y la salud de los trabajadores.

Para la consecución de este objetivo el Consejo de la CEE ha adoptado una serie de Directivas de aplicación progresiva, teniendo en cuenta las condiciones y regulaciones técnicas existentes en cada uno de los Estados miembros. El pasado 12 de junio de 1989, el Consejo adoptó una Directiva relativa a la aplicación de medidas para promover la mejora de la seguridad y la salud de los trabajadores[16], asimismo para el cumplimiento y aplicación de las

---

[15] COM(90) 314 final, DOCE C 277, 5-11-1990.

[16] Directiva 89/391/CEE. En su art. 16 apartado 1.º establece que «a propuesta de la Comisión, basada en el art. 118 A del TCEE, el Consejo adoptara Directivas específicas relativas, entre otras cosas, a los siguientes temas:

- Lugares de trabajo.
- Equipos de trabajo.
- Equipos de protección individual.
- Trabajos con pantallas de visualización.
- Manipulación de cargas pesadas.....

medidas previstas en esta Directiva, el Consejo de la CEE ha establecido la aprobación de otras normas legales de desarrollo[17].

3. Protección de equipos y productos.

En relación con este objeto de protección, en el ámbito comunitario han sido aprobadas las siguientes disposiciones legales:

– Resolución del Consejo de 5 de junio de 1992, relativa al desarrollo de la red digital de servicios integrados (RDSI) en la Comunidad como una infraestructura de telecomunicaciones a nivel europeo a partir de 1993[18].

– Propuesta de Decisión del Consejo en el ámbito de la seguridad en los sistemas de información[19].

– En relación con la protección de las Bases de Datos en particular, la Comisión ha presentado una propuesta de Directiva el pasado 13 de mayo de 1992[20]. Esta propuesta de Directiva pone de manifiesto la necesidad del establecimiento de un marco jurídico estable que permita mantener un ritmo de demanda de estos servicios, debido a la existencia de grandes divergencias y anomalías entre las legislaciones de los Estados miembros, ya que en muchos casos los operadores sólo cuentan con el derecho de obligaciones a la hora de lanzar al mercado sus bienes y servicios.

– Directiva del Consejo de 14 de mayo de 1991, sobre protección jurídica de los programas de ordenador[21]. La redacción de esta Directiva es una consecuencia inmediata del Libro Verde sobre «el derecho de autor y el desafío tecnológico» publicado en junio de 1988[22]. Con ella se aspira a articular una protección jurídica de los programas dentro del conjunto de las medidas comunitarias tendentes a facilitar la libre circulación de los productos. La Directiva concibe la propiedad intelectual en un sentido amplio, comprensivo de formas de propiedad industrial e incluso del Derecho de obligaciones. La Directiva del Consejo pretende una armonización de las legislaciones de los Estados miembros en materia de la propiedad intelectual, independientemente de su instrumentalización efectiva en cada uno de ellos, hoy por hoy, existe ya, a escala comunitaria, una infraestructura en parte constituida por la «opinio iuris» y las normas positivas de algunos estados: Alemania Federal (1985), Francia (1985), Reino Unido (1988). En España

---

[17] Directiva 90/270/CEE de 29-5-1990, referente a las disposiciones de seguridad y de salud relativas al trabajo con equipos que incluyen pantallas de visualización.

[18] DOCE C 158, 25-6-1990.

[19] COM(90) 314 final, presentada por el Consejo el 27 de julio de 1990.

[20] Propuesta de Directiva del Consejo relativa a la protección jurídica de Bases de Datos COM(92) 24 final-SYN 393.

[21] Directiva 91/250/CEE, publicada en el DOCE L 122, 17-5-1991.

[22] El Libro Verde sobre los derechos de autor y el desafío tecnológico, considera diversos aspectos de la influencia en que están ejerciendo sobre la protección de la propiedad intelectual, las nuevas técnicas de reproducción y difusión.

existe una Ley Española de Propiedad Intelectual de 1987[23], la cual otorga expresamente el rango de obra protegida a los programas de ordenador[24]. Esta Ley prevé un período de protección para los programas de ordenador diferente al del resto de obras intelectuales[25]. En cualquier caso los plazos previstos de protección deberán ser adaptados según las modificaciones previstas en la propuesta de Directiva relativa a la armonización del período de protección de los derechos de autor y determinados derechos afines de 23 de marzo de 1992. (Esta propuesta modifica la Directiva, antes mencionada, sobre programas de ordenador[26]).

IV. LEGISLACION SOBRE TELECOMUNICACIONES

Finalmente, en relación con la consecución del Mercado Interior de las Telecomunicaciones, junto con el Derecho originario, establecido en el Tratado de Roma y el Acta Unica Europea, existen un gran elenco de normas de Derecho derivado.

En primer lugar y con carácter general, la Comisión de la CEE publicó en junio de 1987 el Libro Verde para el desarrollo del Mercado Común de las Telecomunicaciones [27] con el fin de promover un debate sobre las futuras condiciones reglamentarias de las telecomunicaciones con vistas al objetivo del Mercado Unico previsto para 1991.

En cuanto a las Directivas aprobadas en materia de telecomunicaciones, pueden señalarse las siguientes:

– Directiva sobre los procedimientos de Información para Normas Técnicas (83/189/CEE, de 28 de marzo). Su objetivo es fijar los mecanismos a seguir por los Estados miembros para la comunicación entre sí de las normas técnicas y a la Comunidad, así como los procedimientos para el establecimiento de normas europeas y de cooperación entre los Estados miembros.

– Directiva sobre la primera fase de reconocimiento mutuo de la Homologación (86/361/CEE, de 24 de julio). Define los requisitos que han de cumplir los equipos terminales con el fin de ser reconocidos en todos los Estados miembros.

---

[23] Esta Ley desarrolla el artículo 20.1 b) de la Constitución Española, que reconoce y protege el derecho a la producción y creación literaria, artística, científica y técnica.

[24] El artículo 10.1 de la Ley menciona expresamente en el apartado f) los programas de ordenador.

[25] El artículo 97 de la Ley prevé un período de protección de los programas de ordenador de 50 años contados desde el primero de enero del año siguiente al de su publicación o creación.

[26] Los antecedentes legislativos de esta propuesta de Directiva lo constituyen el Convenio de Berna para la protección de las obras literarias y artísticas, y la Convención Internacional de Roma sobre protección de los artistas intérpretes o ejecutantes, los cuales únicamente establecían unos períodos mínimos de protección, dejando a los Estados partes la posibilidad de establecer períodos más largos.

[27] COM(87) 290, 30 de junio de 1987.

– Directiva sobre Equipos Terminales de Telecomunicación (88/301/CEE, de 16 de mayo). El campo de aplicación de esta Directiva son las empresas públicas o privadas a las que el Estado conceda derechos especiales o exclusivos de importación, comercialización, puesta en servicio y/o mantenimiento de terminales de telecomunicaciones.

– Directiva sobre Compatibilidad Electromagnética (89/366/CEE, de 3 de mayo).

Esta Directiva es aplicable a todos los aparatos eléctricos y electrónicos, equipos e instalaciones que contengan componentes eléctricos y/o electromagnéticos cuyo funcionamiento pueda crear perturbaciones electromagnéticas.

– Directiva relativa al establecimiento de un Mercado Interior de los Servicios de Telecomunicaciones mediante la realización de una oferta de Red Abierta de Telecomunicaciones (90/387/CEE, de 28 de junio).

Su objetivo es la armonización de las condiciones de acceso y utilización abiertas y eficaces de las redes públicas de telecomunicaciones, y en su caso, de los servicios públicos de telecomunicación.

– Directiva sobre los Mercados de Servicios de Telecomunicaciones (90/388/CEE, de 28 de junio).

Pretende la apertura progresiva del mercado de las telecomunicaciones a la competencia, mediante la abolición de los derechos especiales o exclusivos, así como la adopción de medidas necesarias para garantizar el derecho de todo operador económico a ofrecer dichos servicios.

El Derecho español, en la Ley de Ordenación de las Telecomunicaciones[28] establece en consonancia con los acuerdos internacionales y la normativa comunitaria, las líneas jurídicas básicas a las que han de ajustarse los servicios de telecomunicaciones que son competencia exclusiva del Estado, organizándolos de forma que se garantice el mandato constitucional[29].

---

[28] LOT, Ley 31/1987, de 18 de diciembre. BOE núm. 303, 19-12-1987.

[29] Art. 18.3: «se garantiza el secreto de las comunicaciones y, en especial, de las postales telegráficas y telefónicas salvo resolución judicial».

Art. 149.1.21, relativo a las competencias exclusivas del Estado, entre las que figuran las telecomunicaciones.

Implicaciones de la informática en el ámbito laboral

M.ª PAZ SERRADILLA SANTOS
Abogado

AURELIA TRINIDAD NÚÑEZ
Licenciada en Derecho

TERESA VELÁZQUEZ RODRÍGUEZ
Licenciada en Derecho
(ESPAÑA)

INTRODUCCION

En 1705 Newcomen descubrió la máquina de vapor, motor de la Revolución Industrial que tuvo lugar durante los siglos XVIII y XIX y en la que la introducción de nuevas máquinas, capaces de sustituir el trabajo humano, liberó al hombre en gran parte de los trabajos y rutinas de orden físico. Esto supuso no sólo profundas transformaciones socio-económicas, sino que provocó además el nacimiento de una nueva realidad social con profundas implicaciones en el mundo del trabajo.

No menos importantes son las modificaciones que se están produciendo a raíz de la creación por la Universidad de Harvard en el año 1944 de la llamada Calculadora Automática de Secuencia Controlada (MARK I o ASCC), considerada como la primera computadora. Desde entonces estamos asistiendo a una de las mayores revoluciones de la organización industrial, con la introducción masiva en todos los sectores de las nuevas tecnologías. Podemos definir la historia de las computadoras como una historia de rápidas transformaciones, inusitada irrupción en la economía y profundas repercusiones en la sociedad.

La implantación de la informática es considerada como un cambio tan importante que, aún en contra de la opinión de algunos, se ha llegado a hablar incluso de «revolución informática», en correspondencia con la historia de la industria, o de «era de la información» entre otros nombres.

A semejanza de la revolución industrial, el desarrollo informático libera al hombre del trabajo físico (mediante la introducción de la robótica) pero también de las numerosas cargas intelectuales a que está sujeto en nuestra época.

Los cambios tecnológicos se han introducido prácticamente en todos los ámbitos de la vida, pero con tal celeridad que ha hecho imposible predecir sus efectos. Es patente que la introducción de la informática constituye un avance de gran utilidad; incrementa considerablemente el nivel de productividad, permitiendo la realización de trabajos a menor costo y tiempo. Otros beneficios generados por las computadoras son: mayor satisfacción en el trabajo, tanto a la hora de resolver problemas complejos como de evitar tareas repetitivas y aburridas; nuevas oportunidades de trabajo, con la creación de nuevos empleos en áreas de programación, operación de computadoras y sistemas de información, etc...

Pero, por otra parte también se pueden alegar implicaciones negativas producidas por el desarrollo informático, a saber: reducción de empleo; descualificación profesional, movilidad; problemas físicos y psíquicos, entre los que cuentan, trastornos visuales, problemas músculo-esqueléticos, despersonalización, sentimientos de frustración, etc.

Aunque es importante tener en cuenta estos aspectos negativos, consideramos que no debe rechazarse la incorporación de las nuevas tecnologías, ya que suponen un gran avance técnico, pero siempre que se adopten medidas básicas sobre:

–Garantías de empleo.

–Garantías laborales y profesionales.

–Garantías para la salud laboral de los trabajadores.

–Enriquecimiento del contenido de la tarea.

–Acciones formativas e informativas.

–Reglamentación en aspectos como: características requeridas a los equipos; correcto diseño del puesto de trabajo, condiciones de trabajo, etc.

Opinamos que ante la innovación tecnológica es imprescindible una permanente investigación de todas sus implicaciones en el ámbito laboral y ante la ausencia de normativa específica, se hace obligada la revisión de las vigentes y la creación de nuevas normas, lo suficientemente abiertas para permitir el control inmediato de futuras situaciones.

PRINCIPALES REPERCUSIONES DERIVADAS DEL USO DE LA INFORMATICA EN EL AMBITO LABORAL

El uso de la informática en el ámbito laboral puede tener consecuencias como las expuestas a continuación:

MOVILIDAD FUNCIONAL

Los cambios que conlleva el uso de la informática en el contexto laboral quedan plasmados en lo que se denomina «Movilidad funcional», pues en el seno de una empresa en que se esté presentando un proceso de informatización, ello va a provocar que determinadas labores sean objeto de reestructuración, de tal forma que se modifique, o incluso puede suceder a veces que se suprima, la actividad de uno o más empleados, lo cual trae aparejado una «movilización de puestos», ostensiblemente hacia niveles más trascendentes.

Se entiende por movilidad funcional, el cambio del trabajador a funciones distintas de las que habitualmente desempeñaba, lo que constituye una modificación del contrato de trabajo ya que da lugar a una alteración de uno de los elementos que lo integran, que es «el propio contenido de la prestación».

La movilidad funcional, en cuanto modificación unilateral del contenido objeto del contrato, manifestación del poder directivo del empresario, constituye una excepcional facultad que, por ello, debe ser contemplada restrictivamente y sometida a unas limitaciones. Así asociaciones profesionales, organismos gubernamentales, organismos internacionales de algunos países como Australia, Bélgica, Estados Unidos, Alemania, Japón, han elaborado numerosas normas generales, Repertorios tipo, Disposiciones específicas y Convenios Colectivos, con el fin de proteger al trabajador ante los cambios en sus puestos de trabajo debido al proceso de informatización. Se pretende que todo el personal afectado por el empleo de las nuevas tecnologías conserve su puesto de trabajo y si acaso esto fuere imposible que se le ofrezca otro de similares características e idéntica categoría y sueldo. En ningún momento la introducción del ordenador como medio de trabajo debe suponer un perjuicio para el status laboral del trabajador, pues en la mayoría de los casos son decisiones tomadas por el empresario sin proporcionar a los trabajadores información de cómo esta movilidad funcional les puede afectar, y así la mayoría de las Disposiciones, Convenios, Normas y repertorios vienen a exigir «que se notifique anticipadamente a los trabajadores y a sus representantes

sindicales información sobre los cambios previstos, para que en las decisiones de la dirección puedan tenerse en cuenta las opiniones de los trabajadores; que al mismo tiempo se les suministre información sobre el personal afectado, las modificaciones en la organización del trabajo, las necesidades en materia de formación, las reducciones de personal, los cambios de ocupación, la clasificación de los puestos de trabajo, e incluso en algunos casos, se solicita la creación de Comisiones Conjuntas (dirección/trabajador) u órganos consultivos destinados a evaluar y controlar los efectos de las nuevas tareas sobre los trabajadores o a elaborar normas generales». En España esta materia viene regulada en el artículo 39 del Estatuto de los Trabajadores, que a continuación vamos a analizar. Este artículo preceptúa que «La movilidad funcional en el seno de la empresa, que se efectuará sin perjuicio de los derechos económicos y profesionales del trabajador, no tendrá otras limitaciones que las exigidas por las titulaciones académicas o profesionales precisas para ejercer la prestación laboral y la perteneciente al grupo profesional».

Por derechos económicos del trabajador debe entenderse la totalidad de las percepciones económicas del trabajador derivadas de la prestación de servicios, por ello no cabe incluir entre estos derechos las percepciones extrasalariales, dado que por su carácter indemnizatorio o compensatorio tan sólo se devengan cuando se produce la causa que las motiva (dietas, suplidos, quebrantos, etc...). En principio debe respetarse el anterior nivel retributivo del trabajador, integrado por la cuantía del salario base y los complementos salariales. Por lo que respecta a los complementos personales, de vencimiento periódico superior al mes, en especie, o de residencia, la movilidad funcional no les afecta. Los complementos por cantidad y calidad de trabajo, deben ser mantenidos en su cuantía íntegra, fundamentalmente porque estos complementos remuneran las lógicas consecuencias del grado de profesionalidad, especialización y dedicación del trabajador en el ejercicio de su actividad; por ello no parece razonable que, en los supuestos de movilidad funcional, se ignoren esas cualidades personales y profesionales ya acreditadas, en cuanto supondría una negación del grado de promoción económica alcanzado.

La movilidad funcional se efectuará también sin perjuicio de los derechos profesionales del trabajador. Estos derechos son los derivados de la profesión u oficio que ejerce efectivamente. El trabajador tiene derecho a la libre elección de profesión u oficio y a la promoción a través del trabajo, recogido en el artículo 35 de la Constitución Española. La libre elección se plasma al tiempo de celebración del contrato con el establecimiento de una prestación de servicios determinados que, a su vez, configuran el contenido de una concreta profesión u oficio.

El ejercicio de la profesión u oficio concertada voluntariamente con el empresario, obliga a éste a dar ocupación efectiva al trabajador en una actividad que no difiera sustancialmente con la acordada en su momento.

La promoción a través del trabajo lo es tanto **profesional**, es decir el derecho a acceder a una superior categoría, bien obteniendo una mayor consideración con su trabajo, bien desarrollando una nueva función que lleve implícito un superior reconocimiento, como **económica**; por ello las razonables expectativas de incremento económico han de ser tomadas en consideración en el supuesto de Movilidad Funcional.

En íntima conexión con la promoción a través del trabajo se encuentran la formación y el perfeccionamiento profesionales (art. 22 del Estatuto de los Trabajadores). Ambos se llevan a cabo en mayor o menor medida, a través del ejercicio continuado de la propia profesión u oficio; por ello, la asignación de una labor sustancialmente distinta de la que habitualmente desempeñaba, puede ir en detrimento de la formación permanente del trabajador, por lo que, en tal caso, podría ser ilícita la movilidad funcional. De ahí que el empresario está obligado a facilitar una formación práctica y adecuada a los trabajadores cuando cambien de puestos de trabajo.

El cambio de funciones no puede suponer para el trabajador una limitación de su derecho a la realización de estudios formativos o perfectivos. La movilidad funcional está limitada por las titulaciones académicas o profesionales exigidas para ejercer la prestación laboral.

Asímismo, deberá respetar la pertenencia del trabajador a su grupo profesional. La clasificación profesional se realizará por acuerdo entre el trabajador y el empresario, con sumisión a los términos establecidos en los Convenios Colectivos y, en su defecto, en las normas reglamentarias laborales (art. 16.4 Estatuto de los Trabajadores).

Por clasificación profesional se entiende la asignación de una determinada categoría al trabajador de un grupo profesional, asignación que se efectúa en razón de las funciones concretas a realizar. Por la realización de funciones de otra categoría se respetará, como mínimo el salario correspondiente a la que ostente. El trabajador que realice funciones de categoría superior a las que corresponden a la categoría profesional que tiene reconocida, por un período superior a seis meses durante un año u ocho meses durante dos años, puede reclamar ante la dirección de la empresa la clasificación profesional adecuada.

Después de este análisis podemos apreciar que en los supuestos donde se produzca movilidad funcional por la introducción de la informática en las empresas es perfectamente aplicable esta regulación dentro de ese sector.

CONTRATACION

En el contrato de trabajo del personal informático se deberían incluir de forma específica determinadas claúsulas que en esta materia cobran especial relevancia, dado que el trabajador va a manejar Información Confidencial que por ser tal, es de sumo interés para la empresa; tales claúsulas serán

las relativas al Deber de Buena Fe y Secreto Profesional, el Deber de No Concurrencia, el Pacto de Exclusividad y el Pacto de Permanencia. Tanto trabajador como empresario van a tener que ajustar sus conductas a las reglas admitidas como demostrativas de rectitud y honestidad. El trabajador y empresario han de someter sus prestaciones recíprocas a las exigencias de la buena fe, pues el trabajador tiene como deber básico cumplir con las obligaciones concretas de su puesto de trabajo de conformidad con las reglas de la buena fe y diligencia, deber que alcanza también al empleador o empresario en cuanto es una OBLIGACION MUTUA de lealtad y de honradez propia del contrato de trabajo; es una exigencia de comportamiento ético en el ámbito contractual. La transgresión de la buena fe contractual puede constituir un incumplimiento grave y culpable del trabajador que puede ser causa de despido; así mismo puede ser un incumplimiento grave la transgresión de la buena fe por parte del empresario, pudiendo ser causa justa para que el trabajador solicite la extinción de su contrato con derecho a una indemnización que debería estar igualada a la del despido improcedente.

Las manifestaciones de este deber de Buena Fe son:

–SECRETO PROFESIONAL: El trabajador informático que en el ejercicio de su trabajo va a manejar información confidencial tendrá que estar obligado a mantener los secretos relativos a la explotación y negocios de su empresario, lo mismo durante la vigencia de su contrato que después de su extinción. El incumplimiento del deber de secreto puede llegar a ser muy grave debido a que puede producir a la empresa perjuicios irreparables, por lo que debería estar sancionado con el despido del trabajador, obligándole a indemnizar daños y perjuicios al dueño de la empresa o incluso podría ser castigado por un delito de Revelación de Secretos, tipificado en nuestro Código Penal.

–EL DEBER DE NO CONCURRENCIA: Al trabajador informático se le podría exigir, por razones de seguridad y para evitar perjuicios en la empresa donde va a desarrollar su labor, que durante la vigencia del contrato no pueda efectuar prestación laboral para diversos empresarios cuando tenga que dedicarse a actividades de la misma o similar naturaleza de las que está ejecutando en virtud de su contrato de trabajo, pues es evidente que todo trabajo idéntico o similar, y más aún si se desarrolla en la misma localidad, puede producir tal perjuicio.

Si esta concurrencia desleal se produce se va a considerar como una transgresión de la buena fe contractual, pudiendo llevar aparejado el despido del trabajador, si constituyera un incumplimiento grave y culpable. Una vez extinguido el contrato de trabajo, el empresario y el trabajador están facultados para pactar la no concurrencia de este último, con determinados requisitos de duración, compensación económica, etc.

El empresario que, por interés industrial o comercial, proporcione a sus trabajadores una formación adecuada para desempeñar sus funciones, le va a

interesar que el tiempo y el dinero que ha empleado en ellos le proporcionen un buen rendimiento, y por supuesto la seguridad de que sus trabajadores van a continuar a su servicio y no van a marchar a otras empresas, al menos durante un tiempo prudencial, que podría ser dos años, pues no sería raro que se produjera lo que se suele conocer como «piratería de empleados» yendo en detrimento del empresario que les proporcionó la formación adecuada produciéndole un grave perjuicio; en vistas de esto, en el contrato de trabajo del trabajador informático además de las claúsulas anteriores se podrían incluir las referentes al **Pacto de Exclusividad** y al **Pacto de Permanencia**.

–PACTO DE EXCLUSIVIDAD, o también de plena dedicación, que puede ser concertado entre trabajador y empresario y que impide al trabajador prestar sus servicios en otra empresa aún cuando ello no supusiera concurrencia desleal. En este caso, el trabajador informático tendría derecho como contraprestación a una compensación económica por su plena dedicación.

–PACTO DE PERMANENCIA. En el supuesto de que el trabajador haya recibido una especialización profesional con cargo al empresario para poner en marcha proyectos determinados, como puede ser la informatización de la empresa, podrá pactarse de forma clara y concreta en el contrato, la permanencia en dicha empresa durante cierto tiempo. El pacto de permanencia tendría que tener una duración determinada y el plazo se deberá contar a partir del momento en que finaliza la especialización facilitada al trabajador, sin incluir el período durante el cual se recibe la referida especialización.

Por estos motivos que acabamos de exponer sería aconsejable que, ya desde las Facultades o Escuelas Universitarias, se ofrezca formación sobre deontología profesional, inculcando a los futuros trabajadores informáticos lo importante que puede llegar a ser un comportamiento ético, ajustado a la buena fe, a la honradez, lealtad y rectitud en el desempeño de labores futuras y que redundará tanto en beneficio propio como ajeno.

DESEMPLEO

No cabe duda que el uso de la informática genera empleo; así se han creado nuevas categorías profesionales tales como Técnico de sistemas, Analista titulado superior, Analista de aplicaciones, Analista Programador, Programador y otras, pero como contrapartida y debido a la automatización de actividades quedan vacantes muchos puestos con el consiguiente desempleo, tan negativo para la sociedad.

Se trata de un fenómeno significativo y de grandes repercusiones, ya que los ordenadores y la informática en general han incursionado en todos los ámbitos. Estas repercusiones pueden analizarse desde dos ópticas diferentes:

1. Por un lado, están los despidos que se producen como consecuencia de la inadaptación del trabajador a los cambios tecnológicos introducidos en la empresa.

En este sentido parece necesaria una normativa que proteja a los trabajadores en sus puestos de trabajo. La introducción de nuevas tecnologías no debe suponer una disminución del número de trabajadores fijos en plantilla. Aquellos trabajadores que no puedan adaptarse a estos cambios deben contar con otro tipo de trabajo, sin pérdida de salario, categoría profesional o prestaciones. Numerosas disposiciones estipulan de forma categórica que no se producirán despidos de empleados debido a la informatización de la empresa donde trabajan.

Si se anulan puestos de trabajo debido a la racionalización derivada de la instalación de ordenadores, el empleador debe ofrecer a los trabajadores un empleo equivalente en otro lugar de la empresa. Estos cambios de empleo no deben acarrear ninguna disminución de los niveles acordados de sueldo ni de las sumas adicionales que normalmente se abonan.

Los despidos ocasionados sin tener en cuenta estas medidas podrían ser calificados como improcedentes.

2. Por otro lado, la reducción de empleo provocada por la informática se debe también a una menor contratación debido a una disminución en la necesidad de adquirir mano de obra. Aumentan las facilidades de gestión, con rapidez y seguridad en las labores rutinarias para las que se requería anteriormente un gran volumen de empleados. Se multiplica la actividad comercial y la aplicación de nuevos y creativos métodos en los negocios con una dinámica mayor, con la posible sustitución del hombre por la máquina y una tendencia creciente hacia las fábricas sin trabajadores y las oficinas sin empleados.

El problema, no obstante, puede agravarse si no existe renovación tecnológica ya que, según demuestran los estudios, esto supondría una pérdida de competitividad que desembocaría a medio o largo plazo en un desempleo aún mayor.

CONDICIONES DE TRABAJO

A. JORNADA LABORAL Y PAUSAS DE DESCANSO

Por jornada de trabajo se entiende el tiempo que ha de dedicar el trabajador a la ejecución de su trabajo.

Las primeras fases de la Revolución Industrial se caracterizaron por las jornadas agotadoras, hábito que ha cambiado considerablemente en nuestro días, y aún más, gracias a los avances tecnológicos y a la informatización de las actividades que permiten un incremento de los rendimientos y una reducción del tiempo empleado para conseguirlos.

Es inevitable por tanto, referirse a la organización de trabajo partiendo de estos avances y analizar en qué medida los horarios de trabajo pueden ser modificados, reducidos o limitados.

El uso de ordenadores puede reducir considerablemente el número de horas dedicadas al trabajo con la posible reducción de la jornada. Sin embargo, hay que tener en cuenta que esta reducción puede ser necesaria porque se trata de actividades que generalmente requieren una disposición física y/o mental muy especial y que pueden provocar trastornos en caso de exceso de horas situado frente al ordenador. En este sentido, resultaría muy beneficioso no controlar excesivamente el ritmo y la carga del trabajo, teniendo en cuenta criterios de productividad. Sería conveniente también que el trabajador controle la labor que realiza evitando las tareas repetitivas y monótonas y cualquier factor que contribuya a la creación de tensiones, convirtiéndose en objetivo prioritario la eliminación de motivos que puedan ocasionar dichas tensiones, como única forma de obtener unos resultados óptimos derivados del trabajo con ordenadores.

De todo esto se deriva que no es aconsejable trabajar durante más de cuatro horas seguidas con ordenador y sería positivo la alternancia de esta actividad con trabajos de otro tipo para que las tareas desarrolladas sean creativas y valorizantes.

La mayoría de las disposiciones al respecto recomiendan limitar el trabajo con ordenadores a un máximo del 50% de la jornada laboral, cobrando una importancia considerable el establecimiento de pausas, de modo que el trabajador tenga la posibilidad de efectuar interrupciones habituales para evitar en la medida de lo posible las posturas rígidas, movimientos penosos y fatiga visual.

Generalmente se recomiendan pausas de descanso de diez a quince minutos por cada dos horas de trabajo continuo y se considera bastante conveniente que se tomen fuera del lugar de trabajo (art. 7 de la Directiva 89/391).

B. VACACIONES Y DIAS DE DESCANSO

La sustitución del trabajo por el ocio durante un periodo de cierta duración tiene efectos psíquicos hoy reconocidos como muy saludables. En el caso de trabajadores informáticos es conveniente contemplar que tanto las vacaciones, como los días de descanso, deban ser lo suficientemente satisfactorios como para producir una recuperación física y, en especial, mental en cuanto al tipo de actividad desempeñada.

Al estar sometidos los trabajadores informáticos a unas condiciones que pueden provocarles tensiones, cansancio físico y mental, podría plantearse la posibilidad que tuvieran libertad para elegir el periodo vacacional del que disponen cuando lo consideren más oportuno, ya que en otro caso podría repercutir negativamente en la empresa o lugar de trabajo; incluso sería con-

veniente la concesión de vacaciones o algún día de descanso adicionales, ya que al tratarse de trabajadores que manejan gran volumen de información, en muchos casos confidencial y de gran importancia para la empresa, podrían ocasionar graves trastornos a la misma si desempeñan su trabajo forzadamente y sin el reconocimiento de descansos especiales oportunos.

C. SALARIOS

El salario, que normalmente se fija dependiendo de las circunstancias laborales, presenta particularidades en el caso de los trabajadores informáticos en función de sus características objetivas y subjetivas.

Se trata de una actividad muy cotizada en la actualidad y que puede llegar a poner en tela de juicio el principio de igualdad de salarios ante condiciones laborales idénticas ya que en estas situaciones el salario puede ser diferente por sobrevalorarse en el presente la actividad informática.

FORMACION DEL TRABAJADOR

Los cursos de formación cobran gran importancia, convirtiéndose en la única forma que tiene la empresa para enfrentarse al cambio tecnológico, adaptándose a él y superándolo. Mediante ellos los trabajadores reciben información y conocimientos nuevos y necesarios para mantenerse en sus puestos de trabajo que, debido a la informatización, sufren alteraciones considerables.

Muchas disposiciones se refieren a estos cursos de formación y, en la mayoría de ellas, se establece que debería ser la dirección empresarial la encargada de impartir dicha formación a todos los trabajadores que utilicen ordenadores y también a aquellos cuyos puestos estén indirectamente afectados.

Las condiciones generales de la formación pueden ser negociadas por los sindicatos.

En cualquier caso, es el empleador quien debería sufragar todos los gastos de formación durante el tiempo que sea necesario.

La formación debería referirse a la totalidad del sistema computadorizado y ser lo más adecuada posible para que los trabajadores puedan desempeñar las tareas de una manera competente y en condiciones de seguridad.

Sería conveniente que los cursos de formación fueran considerados como tiempo efectivo de trabajo y se desarrollaran dentro de la jornada laboral, si fuera posible; en caso contrario se abonarían como horas extraordinarias.

En algunas reglamentaciones se especifica la duración conveniente de la formación, variando según los casos, y el momento en el cual debería llevarse a cabo.

Hay que hacer referencia a la labor que la Administración está llevando a cabo mediante el reciclaje de los trabajadores en las tareas informáticas. Se trata de una necesidad planteada en los últimos años para dar la posibilidad al personal de incorporarse a las nuevas tecnologías de la gestión, documentación, información...

DISEÑO ERGONOMICO DEL PUESTO DE TRABAJO INFORMATICO

ERGONOMIA (del griego érgon, trabajo, y nomos, ley norma) es una disciplina que, apoyándose en las investigaciones de la biología y la ingeniería, tiende a lograr la adaptación óptima del trabajo al hombre con el fín de asegurar el máximo de bienestar al factor humano en la vida laboral.

Si para Taylor y sus discípulos lo fundamental era el perfeccionamiento de la máquina y los sistemas de trabajo, sin preocuparse demasiado por las repercusiones humanas de este perfeccionamiento, para la Ergonomía, el punto central de referencia es el hombre, ya que parte del principio de que la máquina puede ser modificada y adaptada a las posibilidades y limitaciones de éste.

Según la OMS existe una estrecha relación entre un mal diseño del lugar de trabajo y la aparición de tensión física y mental que puede repercutir directa y negativamente en el rendimiento y la satisfacción en el trabajo.

Asímismo, el Consejo de las Comunidades Europeas, entre los «Considerandos» que le llevan a adoptar la Resolución 88/C28/01 de 21 de Diciembre de 1987 sobre SEGURIDAD E HIGIENE EN EL TRABAJO indica que «El desarrollo del crecimiento y la mejora de la productividad tanto a nivel de empresa, como a nivel de economía de la Comunidad, dependen, entre otras cosas, de la calidad del medio de trabajo, de las posibilidades que tienen los trabajadores de influir sobre el medio de trabajo con vistas a proteger su salud y seguridad así como de la motivación de estos».

De igual forma, Consejo y Comisión comparten la opinión de que «La protección de la seguridd y de la salud de los trabajadores también debe incluir medidas referentes a la ergonomía en los lugares de trabajo».

Un hecho innegable es que las nuevas tecnologías se han adueñado de nuestra época, pero su incorporación, que supone una amplia modificación de las condiciones de trabajo, se ha hecho en la mayoría de los casos con total ausencia de criterios ergonómicos, como quien coloca una máquina de escribir en la mesa de un empleado.

Así tanto en el ámbito de la ofimática como en otros sectores ha habido quejas por parte de los sindicatos y de los que trabajan con pantallas debido a una falta de adecuación del mobiliario y del ambiente de trabajo a las nuevas máquinas.

Esto ha provocado que organismos gubernamentales, organizaciones internacionales, asociaciones profesionales, institutos de investigación y sindicatos se hayan preocupado en elaborar normas generales y directrices-tipo relativas a factores ergonómicos en puestos de trabajo que incluyen pantallas de rayos catódicos y que van dirigidas principalmente a los representantes de los trabajadores que participan en las negociaciones colectivas, al personal responsable de la selección e instalación de las pantallas y a los trabajadores que las utilizarán.

Estas directrices abarcan aspectos como el diseño de la pantalla, el teclado y el mobiliario; el tamaño y disposición del puesto de trabajo; la iluminación; la temperatura; la humedad y la ventilación; el equipo eléctrico; el control del ruido, las características de las paredes, cortinas, suelo, techo, etc...

Aparte de la existencia de estas normas que han sido incluídas en numerosos convenios colectivos, el Consejo de las Comunidades Europeas ha aprobado en fecha 29 de Mayo de 1990, la quinta Directiva específica con arreglo al apartado 1 del artículo 16 de la Directiva 89/391/CEE. En la misma se considera que los aspectos ergonómicos son especialmente importantes para los puestos de trabajo que incluyen pantallas de visualización y en base a ello, obliga a los empresarios a realizar un análisis de los puestos de trabajo y adoptar las medidas oportunas para paliar los riesgos.

En el Anexo se especifican las disposiciones mínimas que deberán respetar los puestos de trabajo con pantallas y que se refieren a tres apartados concretos:

1. EQUIPO, que incluye:

–Pantalla

–Teclado

–Mesa o superficie de trabajo

–Asiento de trabajo

2. ENTORNO, refiriéndose a:

–Espacio

–Iluminación

–Reflejos y deslumbramientos

–Ruidos

–Calor

–Emisiones

–Humedad

3. INTERCONEXION ORDENADOR/HOMBRE

Como se puede observar, a diferencia de las directrices antes mencionadas, en esta Directiva no se hace alusión a aspectos referentes a las condiciones del local: suelos, ventanales, cortinas, paredes, etc... características muy importantes a tener en cuenta ya que de ello depende también la mayor o menor comodidad de los trabajadores, afectando principalmente a su confort visual.

Por ello se recomienda no utilizar acabados brillantes en paredes, techos y suelos; que los ventanales vayan provistos de persianas, preferiblemente laminillas horizontales regulables; que las superficies acristaladas sean inferiores al 25% de la superficie al sol del local, siendo muy importante que el operador pueda regular en cualquier momento la iluminación.

La Directiva a la que nos hemos referido obliga a los empresarios a adoptar las medidas oportunas para que los puestos de trabajo que en fecha 31-12-92 estuviesen ya en servicio se adapten a las disposiciones mínimas recogidas en el Anexo en un plazo de cuatro años a partir de dicha fecha, y los puestos de trabajo que se pongan en servicio por primera vez después de esta fecha, cumplan estas medidas desde un principio.

Consideramos que es muy importante que las normativas encargadas de regular estos aspectos revistan una naturaleza dinámica y sean susceptibles de ser revisadas con cierta frecuencia a fin de tener en cuenta los últimos hallazgos de la investigación. Así mismo, es importante que tanto los trabajadores como sus representantes sindicales ofrezcan su opinión, participando de algún modo en el diseño ergonómico de su puesto, así como que tengan la posibilidad de acceder a expertos en ergonomía, corriendo la empresa con los gastos correspondientes.

RIESGOS PROFESIONALES. SU PREVENCION

Uno de los más graves problemas, entre los muchos que afectan al mundo del trabajo, y que por ello merece especial relevancia y consideración, es el relativo a los riesgos a que están expuestos los trabajadores en su actividad laboral, ya que constituyen agresiones directas a uno de los derechos fundamentales del trabajador: el derecho a la salud y a la integridad física.

Es incuestionable que debe quedar garantizada la salud en el empleo y para ello es necesario aplicar todas las medidas posibles de prevención y protección en una participación conjunta de autoridades, empresarios, trabajadores y sus representantes. Nuestra Constitución no es ajena a este problema y ordena a los poderes públicos velar por la seguridad e higiene en el trabajo (art. 40.2).

Según el artículo 4.2. del Estatuto de los Trabajadores en la relación de trabajo, los trabajadores tienen derecho «a su integridad física y a una ade-

cuada política de seguridad e higiene» y a tenor de lo dispuesto en el artículo 19.1 «el trabajador en la prestación de sus servicios tendrá derecho a una protección eficaz en materia de seguridad e higiene». El propio trabajador tiene el deber de «observar las medidas de seguridad e higiene» (art. 5º b, ET), punto sobre el que vuelve a insistir el artículo 19.2.

La introducción progresiva de la informática en el mundo laboral incide también de forma directa en aspectos relacionados con la salud en el trabajo, y ello hace imperiosa la necesidad de atender a estas nuevas situaciones, dando respuestas a los nuevos problemas que plantea una sociedad altamente tecnificada en el mundo del trabajo.

Si bien es cierto que frente al endurecimiento masivo de las condiciones de trabajo de otras épocas las nuevas tecnologías incorporan una mejora sustantiva en las condiciones de seguridad, no debemos estar ajenos a los problemas de salud que se han asociado frecuentemente a la introducción de los equipos informáticos.

Aunque hasta el momento no se ha registrado ninguna patología que pueda calificarse como grave, sí que es constatable la aparición de problemas de orden visual, músculo-esqueléticos, alergias y similares, así como stress, fatiga y otros problemas psicológicos (depresión, irritabilidad...) debido a la exigencia, en muchas ocasiones, de máxima concentración, a la monotonía del trabajo, etc., repercusiones que pueden llegar a convertirse en irreversibles.

A este respecto tenemos los estudios que sobre ergonomía informática se han realizado en Suecia (1976), Francia (1978), Alemania (1979), Suiza (1981), y algunos otros países que mencionan los trastornos físicos (irritación de ojos, dolores frontales, miopía, dolores musculares, de columna, hombros, mareos, etc.) y psicológicos (atrofia, fatiga, ansiedad, mecanización, sensación de inutilidad, despersonalización...) que pueden traer consigo el uso de las computadoras.

Una molestia muy dolorosa que se conoce como «síndrome del tunel carpiano» es debida a una falta de relajación de la mano en el teclado o a una altura o inclinación inadecuadas de éste; forma parte de las llamadas lesiones por compresión repetida, que ya han llevado a los tribunales a varios fabricantes de ordenadores en Estados Unidos, ya que puede llegar a inutilizar al trabajador, al limitar de forma grave su coordinación y su habilidad manual.

En el caso concreto de mujeres embarazadas, un estudio realizado en Japón por la Federación de Trabajadores Sohío, ha evidenciado la existencia de afecciones (fatiga, partos prematuros) en aquéllas que desempeñaban sus trabajos con ordenadores.

La Unión General de Trabajadores de España, recomienda en su «Guía Técnica para el trabajo ante pantallas» que mientras no se disponga de prue-

bas irrefutables sobre la seguridad del trabajo con ordenadores, las mujeres embarazadas deberían tener derecho a efectuar otro trabajo.

En cuanto a los temores respecto a posibles riesgos por radiaciones, no existe nada definitivo, aunque se cree que pueden surgir en equipos anticuados; por ello, sería recomendable que se informara con cierta frecuencia a los representantes de los trabajadores o a estos mismos sobre los niveles de radiaciones existentes, con el fin de tomar las precauciones necesarias. Asímismo, para su detección es conveniente una revisión periódica de los equipos por parte de técnicos cualificados.

Como hemos mencionado más arriba, el Consejo de las Comunidades Europeas, en fecha 29 de Mayo de 1990, aprobó la Directiva referente a las disposiciones mínimas de seguridad y salud relativa al trabajo con equipos que incluyen pantallas de visualización. De ella destacaremos lo siguiente: en su artículo 3 obliga al empresario a realizar un análisis de los puestos de trabajo con el fin de evaluar las condiciones de seguridad y salud que ofrecen para sus trabajadores, en particular en lo que respecta a los posibles riesgos para la vista, los problemas físicos y de cansancio mental. En cuanto a la protección de los ojos y de la vista afirma que éstos se «beneficiarán de un reconocimiento adecuado realizado por una persona que posea la competencia necesaria». Se realizarán tanto antes de iniciar el trabajo como de forma periódica posteriormente y cuando aparezcan trastornos que pudieran deberse al trabajo con una pantalla de visualización (art. 9). En el mismo artículo menciona que deberán proporcionarse dispositivos correctores especiales si se demuestra que son necesarios y no pueden utilizarse los normales pero que, «en ningún caso las medidas que se adopten en aplicación del presente artículo deberán implicar cargas financieras adicionales para los trabajadores».

También se concede importancia tanto a la información y formación que deben recibir los trabajadores y sus representantes sobre cualquier medida relativa a la seguridad y salud que se adopte en cumplimiento de la presente Directiva, como a la consulta y participación de los mismos en estos asuntos.

Un aspecto que, a pesar de su importancia, no es recogido adecuadamente en la legislación laboral es el relativo a los problemas psíquicos que puede provocar el trabajo con ordenadores. Si bien, como se ha dicho anteriormente, estudios ergonómicos han constatado la aparición de trastornos psicológicos provocados por el uso de computadoras, no se ha llevado a cabo una regulación que los contemple o que tenga por finalidad su protección o prevención, a pesar de que sus consecuencias pueden ser tan graves como las derivadas de los trastornos físicos. Por ello, considerando que el trabajo no debe suponer un menoscabo en la salud del trabajador en ningún sentido, se hace imprescindible una revisión de la normativa vigente a fin de recoger estos problemas.

INVENCIONES DEL TRABAJADOR. ¿A QUIEN CORRESPONDEN? DERECHOS DE AUTOR. (*)

La aplicación diligente del trabajador en la realización de su trabajo puede dar lugar a unos determinados resultados: descubrimientos, invenciones, creaciones intelectuales..., de especial interés para el empresario.

El problema que abordamos es el que se produce cuando el Programa (Software) es creado en el marco de la relación laboral, que se va a considerar como OBRA AUTORAL y no como Invención, pues su protección en la legislación española viene recogida en la Ley de Propiedad Intelectual, es decir, por la vía de los Derechos de Autor y no por la vía de las Patentes.

El trabajador adquiere un Derecho Moral de Reconocimiento de la Autoría material de la obra que ha creado dentro de su centro de trabajo, ya sea bien durante las horas de trabajo o fuera de ellas. Sin embargo, se va a producir la CESION DEL CONTENIDO PATRIMONIAL DEL DERECHO DE AUTOR, que lo va a detentar el empresario y esta cesión se produce de la manera prevista en el artículo 51 de la Ley de Propiedad Intelectual. Conforme a éste, el empresario sea o no un fabricante de Bienes informáticos, si no ha existido pacto expreso en contrario, adquirirá en exclusiva el Derecho de Explotación del Programa «con el alcance necesario para el ejercicio de su actividad habitual en el momento de entrega de la obra realizada en virtud de dicha relación laboral» (art. 51.2 Ley de Propiedad Intelectual), sin poder disponer de la misma «para un sentido o fines diferentes, pues el Autor no ha procedido a desprenderse de ella de una forma definitiva» (art. 51.3 LPI).

Es así, que la legislación que regula esta materia queda una vía abierta a la posibilidad de que el trabajador al que se le ha reconocido la Autoría Material de la obra, pueda ostentar algún derecho de tipo económico, de compensación salarial de ese trabajo realizado, si existiese un acuerdo con el empresario plasmado por escrito en este sentido. De lo contrario los derechos de explotación van a corresponder en exclusiva al empresario.

La regla general, en materia de cesión de los Derechos Patrimoniales de una creación intelectual, artística o científica, que se contiene en la actual Ley de Propiedad Intelectual Española, es que los contratos de explotación que se refieren a aquéllos no comportan la venta o enajenación de la obra, es decir, no comporta un acto de disposición definitiva; así lo recoge el artículo 43 de la Ley de Propiedad Intelectual. Idénticamente a este precepto, el artículo 2.3 de la Directiva 91/250/CEE, sobre Protección Jurídica de los Programas de Ordenador, prevé que «cuando un trabajador asalariado cree un Programa de Ordenador en el ejercicio de las funciones que le han sido confiadas, o siguiendo las instrucciones de su empresario, la titularidad de los derechos económicos correspondientes al Programa de Ordenador así creado corresponderán, exclusivamente, al empresario, salvo pacto en contrario».

La cesión del contenido patrimonial del Derecho de Autor habrá de efectuarse en documento público e inscribirse en el Registro de la Propiedad Intelectual.

BIBLIOGRAFIA

–DERECHO INFORMATICO. JULIO TÉLLEZ VALDÉS. Universidad Nacional Autónoma de Mexico, 1991.

–TRABAJO CON PANTALLAS DE VISUALIZACION. Oficina Internacional del Trabajo, 1988.

–DERECHO DEL TRABAJO. MANUEL ALONSO OLEA. M.ª EMILIA CASAS BAAMONDE. Universidad Complutense.

–ACTAS DEL X CONGRESO NACIONAL DE MEDICINA, HIGIENE Y SEGURIDAD DEL TRABAJO. (Granada, 14, 15 y 16 de Noviembre de 1984). Instituto Nacional de Seguridad e Higiene en el Trabajo.

–PRACTICA LABORAL. Ediciones Deusto, S.A.

–PUBLICACIONES PERIODICAS DE LA LEY. M.ª DEL CARMEN GETE-ALONSO Y CALERA. Catedrática D. Civil. Universidad Autónoma de Barcelona.(*)

COLOQUIOS

(MESA N.º 7)

INTERVENCION DE D. SANTIAGO RIPOL: Vamos a dar paso a continuación a una sección de preguntas que harían referencia a dos ámbitos de cuestiones, por lo que hemos podido escuchar.

Señalaba Audilio González Aguilar que la informática transforma al Derecho y al jurista, y debemos añadir también que transforma al método docente, como ha puesto de relieve el DR. GONZÁLEZ TABLAS en la exposición anterior, y los planes de estudio son modificados, y el Profesor GALINDO también ha hecho una intervención en este sentido.

Esto sería, por tanto un primer gran bloque de cuestiones que podrían suscitarse, y un segundo bloque, en referencia a lo que hemos escuchado, es que la informática transforma las condiciones de la vida humana. Nos ha hecho referencia en concreto a los problemas que suscita en el ámbito laboral y modifica también las condiciones de vida de los pueblos.

Creo que estas dos cuestiones, o estos dos grandes bloques de cuestiones, se puede dar lugar ya a un debate bastante ámplio.

PREGUNTA: Quería preguntar al Profesor González-Tablas si es muy costoso establecer este sistema de examen.

RESPUESTA DE D. RAFAEL GONZALEZ-TABLAS: Soy Profesor universitario, no me dedico a hacer programas para la venta en el mercado, y en este sentido, la aplicación es un poco rudimentaria, no es un programa comercial, forma parte de una investigación, y habría que depurar el sistema para hacer una aplicación comercial.

SIGUE LA PREGUNTA: Comentándolo con otros compañeros de su Facultad, con respecto a otras asignaturas más complicadas ¿Qué han opinado?

RESPUESTA DE D. RAFAEL CONZALEZ-TABLAS: Siempre se produce la acción perpleja. Filosofía del Derecho o Derecho Natural, en realidad el pensamiento jurídico general, que no es tan puntual como el propio Derecho Positivo, parece tener mayores dificultades de aplicación de procedimientos informáticos.

PREGUNTA: Respecto a la segunda ponencia, DÑA. M.ª PAZ SERRADILLA ha estado hablando de la ergonomía y de los tremendos problemas con que se encuentra hoy el trabajador que tiene que estar delante de un ordenador ocho o diez horas al día, porque vemos como cada vez se respetan menos los derechos del trabajador, que se encuentran recogidos y que nosotros tan vehementemente estudiamos en cuarto de derecho de nuestra carrera, pero tristemente hoy dia en esta sociedad no se cumple, y yo conozco gente que trabaja diez horas al día delante de un ordenador, por un sueldo ridículo, sin respeto ni de los derechos mínimos. Esta es la situación general en las empresas y que no están reconocidos ningún tipo ni de ventajas adicionales.

En concreto quería preguntar por qué un trabajador que es contratado por una empresa, se prevé que lo que él saque, si el saca, por ejemplo, un programa, un software ¿por qué va a ser del empresario? Para eso tenía que ser un técnico super cualificado que ganara mucho más, y fuera expresamente llamado para hacer ese programa. Pero, si una persona como resultado de su trabajo, de su esfuerzo, de estar 15 horas al día, saca un programa, ese es suyo ¿Por qué va a ser del empresario, como dice Vd. que prevé el art. 51.2?

Respecto a lo que ha dicho el Profesor mexicano, es muy triste que realmente el nuevo orden económico mundial que se supone que es bueno, deja que se mueran cien millones de niños al año. Eso es realmente triste y es para reflexionar. Nosotros, europeos, que estamos tam imbuídos de la cultura capitalista, y de lo bueno que es el mercado, habría que pensar un poco más sobre ese tema, y escuchar a las minorías que las diferencias Norte-Sur no sólo son Norte-Sur, sino los «sures» que se crean dentro del Norte, que cada día parece ser que son mayores.

RESPUESTA DE DÑA. MARIA PAZ SERRADILLA: Respondiendo a tu pregunta, he de decir que la obra, el reconocimiento moral lo tiene el trabajador de haber creado esa obra. Lo que el empresario tiene es una cesión del derecho patrimonial de explotación de la obra, pero este artículo deja una vía abierta a que previamente puedan haber pactado trabajador y empresario por escrito, porque tiene que constar por escrito, si no no sirve, el que trabajador va a recibir una compensación económica o una retribución salarial por ese trabajo creado, o sea, que no es que el trabajo, la obra que él va a crear en su puesto de trabajo se va a ceder directamente al empresario para que él pueda disponer de ella de una manera definitiva. El empresario no la va a poder vender ni hacer nada con ella, simplemente va a recoger su contenido patrimonial, lo que obtenga por la explotación de esa obra. Si bien, por escrito, en un pacto entre trabajador y empresario ántes que esta situación se de, pueden acordar que se le reconozca al trabajador una compensación económica por ese trabajo, en caso de que algún día creara una obra intelectual.

PREGUNTA: Mi pregunta va dirigida al DR. GALINDO. Independientemente de la justificación que realiza para que los informáticos puedan recibir

asignaturas que les den un poco más de ética profesional, y algunos valores jurídicos, bajo la consideración de que realmente los informáticos no son más que unos instrumentos para realizar los sistemas, básicamente, ¿no será más importante incidir en incentivar más bien materias informáticas en derecho para que así estos tengan la interfase adecuada para que los sistemas que se vayan a producir sean un reflejo de lo que busca el jurista y no más bien sea el informático el que defina los valores de los sistemas? Básicamente no creo conveniente resaltar exageradamente el poder del informático en la definición de los valores que puedan tener los sistemas.

RESPUESTA DE D. FERNANDO GALINDO: Bueno, los informáticos no son máquinas. Los informáticos son personas, y cuando se contratan con una empresa saben con quién contratan. Yo creo que es conveniente hacerles explícito las distintas convicciones qe están presentes en el Estado en estos momentos, ilustrarles, en fin, un poco acerca de ello, porque, efectivamente, son señores que tienen valores, que no son meros instrumentos, les tengo un gran respeto.

Con respecto al otro tema, efectivamente los juristas tenemos que ser muy conscientes de las tecnologías de la información y la comunicación, sus características y efectívamente, en las Facultades de Derecho hay que explicar esta materia.

Dicho esto, también he de decir lo siguiente. Yo soy profesor de la Universidad de Zaragoza y momentaneamente estoy colaborando en la formación de una nueva Facultad, la Facultad de Derecho de La Rioja, he colaborado en la creación del Plan de Estudios, y ahí he propuesto una asignatura optativa en el plan de estudios de Derecho, en el segundo ciclo, que se titula Informática y Derecho, y que va dirigida a Juristas, pero mi idea inicial es que esta asignatura fuera recibida por informáticos.

He hecho esta asignatura, y mi idea inicial era que fuera para informáticos. Lo que sucede es que por razones operativas, se hace la oferta entre los Profesores de la Facultad de Derecho, y tal vez en estos momentos sea interesante hacer esto, pero al final yo creo que estas asignaturas no tendrán una gran trascendencia en las Facultades de Derecho. Lo más fundamental de las Facultades de Derecho es que se asuman las características de las tecnologías de la información y la comunicación por las diferentes disciplinas, como esta mañana se ha hablado con respecto a Derecho Penal. No hay un nuevo tipo, hay tipos antiguos o hay los tipos habituales de delitos que tienen en cuenta las características de las nuevas tecnologías de la información. Lo mismo sucede con todas las doctrinas, con todas las dogmáticas. Lo importante es que en las Facultades de Derecho, los profesores de Derecho administrativo expliquen fundamentalmente protección de datos u otros temas. Esa es mi convicción. Es decir, de acuerdo con su pregunta, los juristas tenemos que ser conscientes de las tecnologías de la información y la comunicación. Tene-

mos que asumir sus consecuencias en las categorías tradicionales. Esto es lo que sucede en otros países.

PREGUNTA: Yo quería hacerle una pregunta a D. CARLOS DURAND ALCÁNTARA, en cuanto a lo manifestado por él. Es importante y realmente es relevante hacerles llegar los progresos de la informática a esas minorías significativas, como son los indígenas. Lo que me cuestiono es que al mencionar Vd. que esas personas tienen un lenguaje no escrito, sino oral, ¿cómo se adaptará la informática a ese problema en el sentido de que ellos no saben leer ni escribir, según entendí?. No sé si Vds. han ideado alguna solución o han presentado una solución a este problema.

RESPUESTA DE D. CARLOS DURAND: Las áreas de Filología y Lingüística tanto de la Universidad Nacional de México, el actual Instituto Nacional de Investigaciones Antropológicas y otros Institutos de Semiótica, han venido trabajando la codificación y la elaboración de manuales de textos, todo ello aún incluso muchos sin la informática, porque cuando estos estudios se iniciaron datan de la época del Presidente LÁZARO CÁRDENAS DEL RÍO, que creo ha sido el único Presidente del país que realmente protegió los intereses de los campesinos, y que, por cierto, fue quien estuvo muy en contacto con los compañeros republicanos que llegaron en la época de aquella guerra adversa y problemática que tuvo España. Allá tuvimos la oportunidad de recibir a muy grandes intelectuales que crean una gran obra en nuestro país, que fortalecieron nuestras instituciones educativas, y para responder concretamente a su pregunta, hay una gran tarea de gente avocada a la Filología, a la Lingüística, a la Semiótica, a la Hermenéutica, e incluso, ahora que habla el profesor, en el campo de la Filosofía, particularmente, la división de estudios de postgrado. Como estamos trabajando en el doctorado de Antropología, se viene haciendo un buen trabajo al respecto. Es un problema profundo, pero está ese rescate.

Nuestra base tiene que ser el español. Eso lo tenemos que dejar claro porque como ustedes sabrán, estas lenguas que de alguna forma no en el campo propiamente de la informática, pero sí en el campo de la Antropología lingüística, se le ha referido como las lenguas exóticas, entonces de todo eso hay una sistematización, hay un trabajo profundo, anteriormente lo estuvieron haciendo personas ajena, desde el punto de vista de la educación del país. Hubo un decreto de otro Presidente, MIGUEL ALEMÁN, que había permitido al Instituto Lingüístico de Verano, (que es un organismo de los Estados Unidos) elaborar manuales, cartillas, y todo lo que era esta traducción al español de nuestras lenguas índias. Hay dificultades porque en las lenguas indias hay consonantes o letras determinadas que, para pronunciarlas, son guturales, y pareciera que se está diciendo al mismo tiempo varias consonantes seguidas, pero para ellos, es solamente una letra.

No solamente esto, sino los indios, como indios, cómo concebimos los problemas, es decir, cómo entendemos el tratamiento que se debe dar con respecto a las lenguas indias, porque desgraciadamente ha habido un gran aplastamiento de nuestras culturas. Ha habido una falta de respeto de los derechos sociales, económicos y culturales. Entonces es evidente que hoy, y más que hoy, en los 500 años, es una de las grandes reivindicaciones. En un evento tan importante como este, podría ser una de las conclusiones que en la coyuntura de los 500 años es reivindicable ese carácter de pluralidad en el cual se debe ubicar la informática. No en el contexto de la retórica y la demagogia. Sí en el sentido reivindicativo de los derechos de los que, por lo menos allá en mi continente, han sido los propietarios originarios de esos territorios saquedados, vilipendiados, etc., y luego, con todo el respeto, a esta gente tan linda y a España con todo el cariño, no quiero que se pueda concebir de esa manera, sino simplemente hablo de mi historia de las personas indias con que yo trabajo, porque ha sido un poco nuestra investigación y nuestra vinculación con la Universidad. También tenemos algunos libros publicados que hablan de estos datos. En la ponencia que presento vienen las fuentes, incluyendo las oficiales, internacionales que son de organismos serios.

PREGUNTA: Estoy plenamente de acuerdo con el Profesor Galindo en que en las Facultades de Informática haya una asignatura de Derecho Informático o Informática Jurídica. Yo este tema ya se lo he expuesto a algún Decano de Informática. Ahora bien, lo que no estoy de acuerdo es con el contenido. Yo pienso que en la Facultad de Informática debe haber Derecho Informático, igual que en la Escuela de Arquitectura hay Derecho del Urbanismo, como en otras carreras hay Derecho de la especialidad, pero pienso que no tenemos que ir nosotros a enseñar valores. Tiene que ser el propio colectivo el que cree su deontología, su código de valores. Hay una Asociación en la cual participan los informáticos españoles que está tratando de dar un código, pero un código serio. Entonces, pienso que los propios colectivos deben darse su código de valores, y así es mejor aceptado. Si a los juristas nos viniesen a enseñar, por ejemplo los filósofos un código de valores nuestro, inclusive yo creo que lo aceptaríamos mal. Lo que estoy plenamente de acuerdo es que debe haber una asignatura de Informática Jurídica, y que todo lo que está haciendo el Profesor GALINDO en ayuda de la informática jurídica es excelente.

RESPUESTA DE D. FERNANDO GALINDO: Plantea temas escabrosos el tema de los Colegios Profesionales y las éticas, sobre el que no quiero entrar en polémicas. A mí me parece muy bien que los informáticos no tengan Colegios. Es una profesión nueva, sin Colegios. Sus criterios son las leyes.

Yo creo que no hay nada mejor para marcar reglas en un Estado de Derecho que las leyes, porque los códigos deontológicos señalados por una colectividad de señores. ¿Por qué los médicos tienen que tener una serie de

códigos deontológicos que amparan una serie de operaciones y una serie de actividades? Yo creo que se pueden explicar los contenidos de las leyes.

PREGUNTA: Mi pregunta va dirigida al Profesor Galindo y está relacionada con el tema que ha planteado el anterior interviniente en el público, y es el problema de la Autorregulación. Realmente desde una mentalidad jurídica plantea diversos problemas porque si se deja la autorregulación, aunque ahora con su intervención parecía que la rechazaba, o la dejaba de lado, los problemas de quién fija, quién aprueba esas normas, ¿Qué valor tienen? ¿Son normas sociales? ¿Son normas deontológicas? ?Qué sucede en caso de incumplimiento? ¿Va a ser objeto de sanción? ¿Régimen disciplinario de colegios profesionales?. Y una segunda cuestión relacionada con esta, es el papel o la función que cumplen los informáticos, teniendo en cuenta que es muy difícil encontrar el informático aislado, que trabaja como consultor privado. Normalmente estará siempre integrado en una organización pública o privada, y ahí sí que asumirá los valores de esta organización. Si es pública, normalmente una mentalidd en cierta medida burocrática, bien sea su vinculación de Derecho Laboral o una relación de Derecho Administrativo. Si trabaja en una organización privada, hay que pensar que los valores vendrán definidos en primer lugar por el contrato de trabajo, por su vínculo laboral con esa empresa, porque normalmente no va a desarrollar análisis de procesos o procedimientos por su cuenta, sino que será la cuenta de clientes que le marque el empresario.

RESPUESTA DE D. FERNANDO GALINDO: Yo simplemente planteo algo que los juristas tenemos que plantearnos, porque se ha hablado de las Leyes Orgánicas de Regulación de Tratamiento de Datos, y yo simplemente voy a leer el art. 31. 1 del Anteproyecto de la LORTAD española: «Mediante acuerdo sectorial o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular los códigos tipo. Los códigos tipo tendrán el carácter de Códigos Deontológicos o de buena práctica profesional», es decir, nos gustará, será anti-jurídico, no sé lo que será, pero que este tema es un tema actual y de gran importancia en los países donde hay disposiciones de este tipo, eso es cierto.

PREGUNTA: A mí, a la luz de todo esto se me ocurren un par de reflexiones y una pregunta. Entrando en este tema, yo creo que no se trata que los juristas queramos imponerle un código de conducta, ni una «lex acti» profesional a otros colectivos, pero tampoco se trata de un corporativismo a ultranza. El Derecho no es sólo una técnica para resolver conflictos. También es una coordinación ética entre las personas, y esos valores están, por ejemplo, en la Constitución, entonces, alguien tiene que interpretar esos valores. Alguien tiene que decirle a un informático qué es la desobediencia técnica y qué es el deber de obediencia de un trabajador, que de esto saben más los

laboralistas que yo, y cuándo tiene que desobedecer un informático una orden ilegítima, porque puede ser perjudicial para su propia integridad física o psicológica, o para los derechos o libertades de una tercera persona. No es que pretendamos nosotros imponerle nuestra ética a nadie, pero sí creo que algún papel tendremos que jugar.

En cuanto al tema que se ha visto antes de laboral, yo creo que lógicamente el tiempo le ha impedido a la Profesora que nos ha presentado la Comunicación, por la cual la felicito, que quedara bien claro el asunto de la propiedad intelectual, que es otra de mis grandes aficiones. Esta normativa de la ley de Propiedad Intelectual, ha sido siempre muy discutida. Yo creo que no se trata de decir que es que siempre el derecho de explotación es para el empresario. Una cosa es cuando un empresario encomienda a un trabajador que cree un programa –ese es el objeto del trabajo–, y otra cosa, y ahí está el problema, es cuando el trabajador, en horas de trabajo y utilizando medios de su empleador, crea un programa que luego pretende que no tenga en ningún momento facultad de distribuirlo o de explotarlo su empresario, que ahí es donde se plantean siempre las guerras, porque el Código Civil lo dice muy claro, que la renuncia a los derechos habrá de ser expresa, y nunca es una renuncia que se pueda presumir. Lo que sucede es que el mecanismo no es tan simple como la norma, es un poco más complicado cuando se llega al casuísmo.

La edición de este volumen ha sido posible gracias a la colaboración especial de Editorial Aranzadi, S. A.

ARANZADI
EDITORIAL

UNESCO

JUNTA DE EXTREMADURA