Universitat Oberta de Catalunya

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

MONOGRÁFICO

III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas

Agustí Cerrillo, Jordi García y Mònica Vilasau (coord.)

Sumario

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

Presentación

Los días 7 y 8 de mayo del 2007 tuvo lugar en Barcelona el III Congreso anual «Internet, Derecho y Política (IDP)» (http://www.uoc.edu/symposia/idp2007/esp/index.html). Un año más, la Universitat Oberta de Catalunya, desde sus Estudios de Derecho y Ciencia Política, reunió a un centenar de académicos, profesionales y estudiantes para reflexionar conjuntamente en torno a las respuestas que desde los ámbitos jurídico y político se están dando para hacer frente a los retos y aprovechar las oportunidades derivadas del uso masivo de las tecnologías en todos los ámbitos de la vida social.

La 3.ª edición del Congreso IDP contó con diferentes paneles dedicados al *copyright*, la protección de datos, la seguridad en la red, los problemas de responsabilidad, el voto electrónico, la regulación de la administración electrónica y el análisis del estado del uso de las TIC por parte de los profesionales del derecho. Una de las novedades de esta tercera edición fue la celebración, en el marco del Congreso, de una jornada profesional, que tuvo como objetivo la reflexión, el debate y la discusión más intensiva sobre problemáticas y realidades de colectivos profesionales concretos: en este caso se dedicó a la protección de datos en la Universidad y se dirigió principalmente a todos los profesionales responsables o técnicos de la protección de datos en el entorno mencionado.

En este monográfico, aparte de una presentación general de los temas discutidos en los diferentes paneles, se recogen algunas de las ponencias más relevantes presentadas en las sesiones sobre responsabilidad de los intermediarios, protección de datos y seguridad en la red. También encontraréis la reseña de la mencionada jornada profesional y las dos comunicaciones que fueron premiadas *ex aequo* en este congreso.

En la clausura del congreso se puso de relieve cómo la revolución de las tecnologías de la información y comunicación no ha hecho más que empezar y, por lo tanto, hace falta una nueva forma de entender tanto el derecho como la política. En este monográfico encontraréis una amplia muestra de las aportaciones presentadas. Esperamos que, de nuevo, sean del interés del lector.

Agustí Cerrillo, Jordi García y Mònica Vilasau
Coordinadores del monográfico
Profesores de los Estudios de Derecho y Ciencia Política de la UOC

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

«Sólo sé que no sé nada (efectivamente)»: la apreciación del conocimiento efectivo y otros problemas en la aplicación judicial de la LSSI

Miquel Peguera Poch

Fecha de presentación: junio de 2007
Fecha de aceptación: julio de 2007
Fecha de publicación: septiembre de 2007

Resumen
Este trabajo está concebido como *working paper* y lleva a cabo un análisis de la aplicación judicial de las reglas de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico en materia de responsabilidad de los prestadores de servicios de intermediación. En los cinco años de vigencia de la ley, las resoluciones dictadas son todavía pocas, pero se han planteado ya conflictos de variada tipología. Uno de los puntos más conflictivos en la interpretación de estas normas es el sentido que deba darse al requisito de carecer de conocimiento efectivo para poder gozar de la exclusión de responsabilidad en los casos de alojamiento de datos y en los supuestos de provisión de enlaces. La interpretación de este punto ha sido claramente divergente en las resoluciones judiciales que conocemos. El trabajo presta especial atención a este problema, y analiza también otros, como son el relativo a la admisibilidad de acciones de cesación y el problema más elemental de la inaplicación pura y simple de la ley.

Palabras clave
LSSI, responsabilidad, ISP, intermediarios, comercio electrónico, exenciones, conocimiento efectivo

Tema
Responsabilidad de los ISP

"I just know that I know nothing (actually)": the finding of actual knowledge and other problems within the judicial application of the LISS (Law on Information Society Services).

Abstract

This work is designed to be a working paper and undertakes an analysis of the legal application of the rules set forth in the Law on Information Society and e-Commerce Services as regards the liability of intermediary service providers. In the five years since the law came into force, few decisions have been issued, although various types of conflicts have been considered. One of the most conflictive points when interpreting these rules is the sense that must be given to the requisite of lacking actual knowledge to be able to enjoy exclusion from liability in cases of data storage and link providing. The interpretation of this point has clearly been divergent in the judicial decisions of which we are aware. The work pays special attention to this issue, as well as analysing others, such as that relating to the admissibility of injunctions and the more basic problem of the pure and simple non-application of the law.

Keywords

LISS, liability, ISP, intermediaries, e-commerce, exemptions, effective knowledge

Topic

Liability of ISP

Introducción

Se cumplen ahora cinco años desde la entrada en vigor de la Ley de Servicios de la Sociedad de la Información (LSSI).[1] La Ley, que poco después de su aprobación ya fue modificada en dos ocasiones,[2] está a punto de ser nuevamente reformada a través del Proyecto de Ley de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones,[3] y sobre todo mediante el Proyecto de Ley de Medidas de Impulso de la Sociedad de la Información.[4]

Estas últimas modificaciones de la LSSI afectan directamente a la actividad de los intermediarios técnicos de la red, o por decirlo en el lenguaje de la ley, de los prestadores de servicios de intermediación de la sociedad de la información, esto es, de quienes prestan servicios como los de acceso y transmisión de datos (con o sin copia en caché de los mismos), o bien de alojamiento de información, o de provisión de enlaces o de instrumentos de búsqueda de contenidos en la red. Sin embargo, estas reformas –salvo en un pequeño punto de importancia menor–[5] no modifican el texto de los artículos 13 a 17 de la LSSI, esto es, las reglas que tratan de la res-

1. Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (BOE n. 166, de 12 julio de 2002). La Ley entró en vigor el 12 de octubre de 2002.
2. La primera modificación se obró en virtud de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (BOE n. 264, de 4 de noviembre), y la segunda tuvo lugar poco después en virtud de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (BOE n. 304, de 20 de diciembre). Una versión actualizada de la LSSI puede consultarse en http://civil.udg.es/normacivil/estatal/contract/LSSI.htm
3. Actualmente en el Senado; *vid*. http://www.senado.es/legis8/publicaciones/html/textos/II0108A.html
4. En fase de tramitación parlamentaria en el Congreso: *vid*. BOCG, Congreso de los Diputados, serie A, 11 de mayo 2007, núm. 134-1. Disponible en http://www.congreso.es/public_oficiales/L8/CONG/BOCG/A/A_134-01.PDF
5. Me refiero a la reforma prevista del artículo 17.2 LSSI.

ponsabilidad de dichos prestadores. Como es sabido, en dichos artículos el legislador delimita una serie de supuestos de hecho garantizando que, si se cumplen las condiciones previstas en los mismos, el prestador del correspondiente servicio de intermediación no podrá ser declarado responsable de los contenidos ilícitos de terceros que dicho prestador haya transmitido, alojado o enlazado.

Estas previsiones, destinadas a garantizar un umbral mínimo de exclusión de responsabilidad para los intermediarios, constituyen la incorporación a nuestro derecho interno de lo dispuesto en los artículos 12 a 14 de la Directiva sobre el Comercio Electrónico (DCE),[6] con la adición de una exclusión de responsabilidad no prevista en la directiva, referida a las actividades de provisión de enlaces y de herramientas de localización de información (art. 17 LSSI). No es mi intención exponer ahora el contenido de estos preceptos, bien conocidos ya en la doctrina. El propósito del presente artículo es llevar a cabo un análisis de la aplicación judicial de las citadas reglas de exclusión de responsabilidad a partir de las decisiones judiciales que se han dictado en esta materia. En efecto, contamos ya con algunas resoluciones judiciales que han abordado, si bien de forma desigual, el problema de la responsabilidad de los intermediarios por contenidos de terceros. Sin embargo, los cinco años de vigencia de la ley no han sido suficientes para dar lugar a un cuerpo de doctrina claro y coherente en la aplicación de las normas de exclusión de responsabilidad de la LSSI; ni tampoco para disponer de un conjunto de decisiones lo bastante numeroso como para indicar con precisión una determinada tendencia en la interpretación de dichas normas.

A pesar del escaso número de resoluciones judiciales de que disponemos, la tipología de las situaciones de intermediación contempladas en las mismas es ciertamente variada. Así, han llegado ya a los tribunales conflictos relativos a la actividad de provisión de acceso y transmisión de datos; también reclamaciones por la actividad de suministro de enlaces a contenidos ilícitos; y sobre todo, supuestos de responsabilidad por alojamiento de datos. En esta última categoría contamos no sólo con decisiones que contemplan la actividad básica de los prestadores de *hosting*, esto es, el alojamiento de sitios web, sino también con resoluciones judiciales que abordan el problema de la responsabilidad de otros tipos de alojamiento, como son el de comentarios de terceros en un blog, el de artículos en un wiki, o el de mensajes en un foro. La particularidad de estas situaciones estriba en que el alojador a quien se reclama la responsabilidad no es el proveedor del *hosting* del sitio web, sino el titular o administrador del correspondiente blog, wiki o foro, quien, en la medida en que está alojando datos suministrados por terceros, realiza una función subsumible en el supuesto general de alojamiento de datos contemplado en el artículo 16 de la LSSI.

Las resoluciones judiciales recaídas distan de ser homogéneas. Una primera línea divisoria puede trazarse entre las decisiones que tienen en cuenta la LSSI y aquellas que simplemente parecen ignorar su existencia. Y entre las primeras, los problemas fundamentales de interpretación de las reglas de exclusión de responsabilidad de la LSSI han consistido, por una parte, en la determinación de si la exclusión de responsabilidad en el caso de mera transmisión y provisión de acceso (art. 14 LSSI) impide el ejercicio de acciones de cesación contra el intermediario y, por otra parte, en el significado que debe darse al requisito de falta de conocimiento efectivo de la ilicitud de los contenidos en los supuestos de alojamiento de datos y de provisión de enlaces (arts. 16 y 17 LSSI), punto sobre el que se han adoptado interpretaciones claramente divergentes.

1. El brillo fulgurante de la ausencia

Como apuntábamos, no han faltado resoluciones que han ignorado por completo la existencia de una previsión legal específica dirigida a excluir la responsabilidad tanto civil como penal de los intermediarios. En este grupo podemos citar tres sentencias, todas referidas a supuestos de alojamiento de datos: la Sentencia de 30 de junio de 2006 del Juzgado de Primera Instancia e Instrucción núm. 5 de Arganda del Rey (caso Mafius Blog), que condena al titular de un blog por una falta de injurias y otra de amenazas; la Sentencia de 19 de diciembre de 2006 del Juzgado

6. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el Comercio Electrónico, DCE), DOCE núm. L 178, de 17 de julio de 2000.

de Primera Instancia número 52 de Madrid (caso Frikipedia), que declara responsable al administrador del wiki Frikipedia de una intromisión ilegítima en el honor de los demandantes y le condena a indemnizar a los actores; y por último, la Sentencia de Primera Instancia del caso Sgae contra Asociación de Internautas (sentencia de 15 de junio de 2005, del Juzgado de 1.ª Instancia número 42 de Madrid), que condena a la Asociación de Internautas como responsable de atentado contra el honor de los demandantes por alojar un sitio web de contenido injurioso.

Ciertamente, es posible que en estos casos el juez haya estimado que la exclusión de responsabilidad del artículo 16 LSSI no resultaba aplicable, bien por entender que el supuesto de hecho no era subsumible en dicha norma, bien por considerar que no se cumplían los requisitos exigidos en la misma. Pero lo cierto es que en las sentencias no sólo no se justifica la inaplicación de la regla de exclusión, sino que ni siquiera se hace la más mínima mención a su existencia.

En los tres casos se hace responsable al demandado de unos contenidos elaborados por terceros. En el caso del blog de Mafius, y por lo que ahora interesa, la sentencia considera que el titular del blog (un alumno de un instituto que mantenía un blog crítico con la institución) es responsable, en concepto de autor, de una falta de amenazas por las expresiones contenidas en un comentario enviado al blog por un tercero no identificado.[7]

La sentencia se basa en la jurisprudencia del Tribunal Supremo y del Tribunal Constitucional para considerar que la participación del acusado en los hechos lo fue en concepto de autor. A este propósito, tenemos la Sentencia del TC 200/1998, de 14 de octubre, en cuyo fundamento jurídico 2.º se indica:

> «Por otra parte, en anteriores Sentencias (SSTC 15/1993 y 336/1993) ya nos hemos referido con mayor detalle las consecuencias que tienen lugar "al autorizar la publicación de un escrito ajeno cuyo autor se ha identificado previamente (pues) será éste quien asuma la responsabilidad que del mismo pueda derivarse si su contenido resulta lesivo del derecho al honor de una tercera persona. Sin embargo, la situación es muy distinta si el escrito ajeno es publicado sin que el medio conozca la identidad de su autor, pues en tal supuesto dicho escrito no constituye una acción que pueda ser separada de la de su publicación por el medio, conforme a la doctrina expuesta en la STC 159/1986. De suerte que, al autorizar la publicación del escrito pese a no conocer la identidad de su autor ha de entenderse que el medio, por ese hecho, ha asumido su contenido. Lo que entraña una doble consecuencia: En primer lugar, que el ejercicio de las libertades que el art. 20.1 reconoce y garantiza habrá de ser enjuiciado, exclusivamente, en relación con el medio, dado que el redactor del escrito es desconocido. En segundo término, que al medio le corresponderá o no la eventual responsabilidad que pueda derivarse del escrito si su contenido ha sobrepasado el ámbito constitucionalmente protegido de la libertad de información y en su caso de la libertad de expresión lesionando el honor de terceras personas o, por el contrario, la ha respetado" (STC 3/1997 [RTC 1997\3], fundamento jurídico 3.º).»

La sentencia del caso que nos ocupa, tras citar esta STC, declara lo siguiente:

> «La citada doctrina, avalada por otras sentencias (SSTC 41/1994, de 15 de febrero, 336/1993 de 15 de noviembre y 3/1997, de 13 de enero, y las SSTS 5-12-1989, 4-10-1988 y 16-5-1991) impone, pues, la necesidad de cerciorarse de la identidad del autor del escrito que se va a publicar, para derivar a éste la responsabilidad, ya que, si el escrito se publica sin que el medio (en este caso el editor) conozca aquella identidad, en tal supuesto dicho escrito, como antes se dijo, no constituye una acción que pueda ser separada de la de su publicación por el medio, ya que, entonces, el medio (autor) asume su contenido y la subsiguiente responsabilidad. Conforme a dicha doctrina la autoría de D. (....) en este caso no ofrece dudas, a la vista de los arts. 27, 28 y 30.2,1.º, del Código penal, sin que puedan servirle de cobertura para la exención de la responsabilidad penal cláusulas de salvaguarda, que en el presente caso no existen, siendo así que el propio editor en el acto manifestó que había programado el blog para que se omita el apartado donde se recoge la dirección de IP, lo que ha puesto de manifiesto en el citado blog reiteradamente como salvaguarda de impunidad.»

Al margen del problema de si esta doctrina es de aplicación al caso de un blog, y en particular si lo dispuesto en el artículo 30 CP para los «medios o soportes de difusión mecánicos» es aplicable a un medio como Internet, el problema que queremos destacar aquí es la ausencia de toda consideración al artículo 16 LSSI, en el que podría encontrarse una exclusión de la responsabilidad del blog.

Inicialmente, son dos los obstáculos que podrían oponerse a la aplicabilidad de dicho precepto. El primero es el interrogante sobre si la exclusión de responsabilidad prevista en el mismo alcanza a excluir no sólo la responsabilidad civil sino también la penal. La respuesta aquí entiendo que debe ser positiva, a pesar de que en la norma no se declara de modo explícito. Ya en

7. Por dicha falta se le condenó a la pena de veinte días de multa a razón de diez euros diarios. A la misma pena se le condenó por una falta de injurias, ésta en razón de un post escrito por el propio *blogger*. Este último punto, sin embargo, no resulta relevante para nuestro análisis, puesto que es claro que respecto de contenidos propios no es aplicable la exclusión de responsabilidad. El condenado fue absuelto en apelación de la falta de amenazas.

la directiva es claro que la exclusión de responsabilidad cubre también la de carácter penal, y así lo ha destacado la doctrina.[8] Por otra parte, así se indica claramente en el comentario de los artículos que acompaña la propuesta inicial de la DCE,[9] y en el mismo sentido se pronuncia el primer informe sobre la aplicación de la directiva.[10] En la LSSI no hay tampoco una declaración expresa que establezca este alcance, pero parece claro que éste es el objetivo de la norma, que sigue el sentido de la directiva, y así lo ha señalado la doctrina penalista.[11]

El segundo obstáculo se refiere al ámbito de aplicación material de los artículos 13 a 17 LSSI, que se limita a determinadas actividades de intermediación que deben reunir los requisitos generales que definen la noción de «servicios de la sociedad de la información», entre los que se halla el de que se trate de un servicio prestado normalmente a título oneroso, esto es, que se trate de una actividad de carácter económico.[12] Parece claro que este elemento de onerosidad no se daba en el caso de autos, puesto que el blog no constituía una fuente de recursos, o al menos no consta. Sin embargo, la concesión de la exclusión de responsabilidad en los casos de actividades económicas y la denegación de la misma a las actividades no lucrativas resulta problemática, ya que la nota del carácter económico no guarda relación alguna con el fundamento de la concesión de la exclusión de responsabilidad, que se halla en el carácter neutro y pasivo del intermediario. Esta dificultad, pues, podría probablemente resolverse acudiendo a la aplicación analógica de la norma para reconocer la exclusión de responsabilidad también a aquellos supuestos en que la actividad no reviste carácter económico.

Salvados estos dos primeros obstáculos, sería preciso valorar todavía, si el hecho de alojar un comentario enviado por un lector del blog supone que el titular del blog está llevando a cabo un servicio de intermediación de alojamiento de datos, que es el supuesto previsto en el artículo 16 LSSI. Como ya apuntaba al principio, pienso que, en efecto, al estar alojando unos datos que han sido suministrados por terceros, el titular del blog, como el de cualquier sitio web, lleva a cabo una actividad de alojamiento que encaja en el supuesto del artículo 16 LSSI. Este artículo no debe entenderse referido exclusivamente a la actividad de *hosting* de sitios web, sino a cualquier supuesto de alojamiento de datos suministrados por terceros. En cuanto a la directiva, este sentido amplio del supuesto de hecho de alojamiento de datos (art. 14 DCE) resulta confirmado en el primer informe sobre la aplicación de la directiva, al señalar que «[e]n particular, la limitación de la responsabilidad por el alojamiento de datos, prevista en el artículo 14, abarca diferentes supuestos de almacenamiento de contenidos ajenos, aparte del alo-

8. *Vid*., entre otros, Emmanuel CRABIT (2000). «La directive sur le commerce électronique. Le projet Méditerranée». *Revue du Droit de l'Union Européenne*. N.º 4, pág. 749-831, esp. pág. 777-778; *vid*. también Mario E. CLEMENTE MEORO (2003). «La responsabilidad civil de los prestadores de servicios de la sociedad de la información». En: Mario E. CLEMENTE MEORO y Santiago CAVANILLAS MÚGICA. *Responsabilidad civil y contratos en Internet. Su regulación en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*. Granada: Comares. Pág. 1-116, esp. pág. 74.
9. COM (1998) 586 final, Bruselas, 18.11.1998. En el documento COM, la propuesta de directiva se acompaña de una extensa exposición de motivos así como de un anexo de comentarios individualizados artículo por artículo. En la versión publicada en el Diario Oficial tan sólo se reproduce el texto articulado de la propuesta (n. C 30, de 5 de febrero de 1999, pág. 4.).
10. COM (2003) 702 final, Bruselas, 21.11.2003, pág. 14.
11. Sobre la aplicabilidad de las reglas de exclusión de la LSSI a la responsabilidad penal, puede verse, entre otros, Óscar MORALES GARCÍA (2001). «Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información». *Revista de Derecho y Proceso Penal*. N.º 3, pág. 139-167; y Javier GUARDIOLA (2004). «Limitaciones a la responsabilidad penal de los prestadores de servicios de la sociedad de la información: eficacia en el ámbito penal de las exenciones previstas en la Ley 34/2002». En: Miguel Ángel DAVARA (coord.). *XVIII Encuentros sobre Informática y Derecho 2003-2004*. Madrid: Universidad Pontificia de Comillas. Este último señala que «es posible entender que los supuestos de exención de responsabilidad previstos en los arts. 14 a 17 de la LSSI responden, en realidad, a la concurrencia de causas de justificación que se integran en el ámbito penal de la mano de la previsión de la eximente de ejercicio legítimo de un derecho del art. 20.7.º del Código penal. Y, por ende, quien actúa en su ámbito queda exento de responsabilidad penal»; *vid*. también Manuel GÓMEZ TOMILLO (2006) (2.ª ed.). *Responsabilidad Penal y Civil por Delitos Cometidos a través de Internet. Especial consideración del Caso de los Proveedores de Contenidos, Servicios, Acceso y Enlaces*. Navarra, Cizur Menor: Aranzadi.
12. *Vid*. el anexo de definiciones de la LSSI, letras a) y b). *Vid*, asimismo, el apartado II de la Exposición de Motivos de la LSSI. *Vid*. también el artículo 2.b) de la Directiva sobre el Comercio Electrónico, y el artículo 1.2) de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE.

jamiento de sitios web, por ejemplo, tablones de anuncios electrónicos o salas de charla ("chat-rooms").»[13]

Finalmente, habría que analizar si el titular del blog reunió los requisitos específicamente previstos en el artículo 16, esto es, carecer de conocimiento efectivo de la ilicitud de los materiales, y en caso de tener dicho conocimiento, proceder a la retirada del material. No vamos a abordar aquí estos extremos. Simplemente queremos dejar constancia de que probablemente la sentencia debería haber examinado el artículo y haber justificado, en su caso, el motivo de su no aplicación.

El segundo ejemplo que citábamos de completa inaplicación de la LSSI es la sentencia del Juzgado de Primera Instancia número 52 de Madrid, de 19 de diciembre de 2006.[14] En este caso, el demandado era el administrador de un wiki denominado Frikipedia, una suerte de recreación satírica de la conocida Wikipedia. En una de las voces (no elaborada por el administrador de la página, sino colaborativamente por los usuarios, como es propio de un wiki), concretamente voz referida a la SGAE, se contenían expresiones injuriosas y atentatorias contra el honor. La sentencia declaró que se trataba de «expresiones insultantes, de parte de grave menosprecio que no son tolerables en la convivencia social», y a pesar de que el demandado ya había retirado dicho contenido una vez que tuvo conocimiento de la acción ejercitada, le condenó a indemnizar a los actores con un importe total de seiscientos euros, justificando la atribución de responsabilidad al administrador de la página con el argumento de que «se declaró acreditado –por las actuaciones reiteradas en juicio– que [el demandado] tenía facultad para dirigir o no la página, es decir, las opiniones que entraban o no.» (F.J. 2.º).

En cuanto a la posibilidad de aplicar la exclusión de responsabilidad prevista en el art. 16 LSSI, cabe plantear el mismo problema que en el caso anterior, esto es, el de si se trataba o no de una actividad económica. En este caso, la presencia de publicidad en la página hace pensar que sí podría calificarse de actividad económica. También debería resolverse en sentido afirmativo, en mi opinión, la pregunta sobre si el alojamiento de unos contenidos que han sido elaborados por terceros –los usuarios del wiki– resulta subsumible en el supuesto de hecho de servicio de intermediación de alojamiento de datos previsto en el artículo 16 LSSI. Estos problemas, sin embargo, no son tratados en la sentencia, en la que simplemente no aparece ninguna mención a la LSSI.

El tercer ejemplo de resolución judicial en que la LSSI brilla por su ausencia es la sentencia de primera instancia del caso de la SGAE contra la Asociación de Internautas (sentencia de 15 de junio de 2005, del Juzgado de 1.ª Instancia número 42 de Madrid). Trataremos este caso más abajo, puesto que la sentencia de apelación, que confirma la de instancia, sí hace referencia a la LSSI, y resulta de interés para analizar el problema de la apreciación del conocimiento efectivo.

2. La discusión sobre la admisibilidad de acciones de cesación contra proveedores de acceso

Otro punto relevante para el análisis de la aplicación judicial de la LSSI es el relativo a la admisibilidad de acciones de cesación frente a determinados proveedores de servicios de intermediación. Como es sabido, la DCE, advierte expresamente, para cada una de las exclusiones de responsabilidad, que dicha exclusión «no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados Miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida».[15] Es claro, pues, que tal como están concebidas en la directiva, las exclusiones de responsabilidad no limitan la posibilidad de ejercitar acciones de cesación contra el proveedor si éstas están contempladas en el ordenamiento del Estado Miembro. Esta indicación expresa de que la exclusión de responsabilidad no afecta al ejercicio de acciones de cesación, sin embargo, no aparece en los artículos de la LSSI. El legisla-

13. COM (2003) 702 final, pág. 14, nota 64. En términos parecidos se expresa el comentario de los artículos que acompañan la propuesta de Directiva: COM (1998) 586 final.
14. La sentencia fue recurrida en apelación y no tengo noticia de si se ha dictado ya sentencia.
15. *Cfr*. art. 12.3 de la Directiva sobre el Comercio Electrónico, y en términos prácticamente idénticos los arts. 13.2 y 14.3 de la misma directiva.

dor español consideró probablemente que no era necesario declararlo de modo expreso. Lo que en ningún caso cabe entender es que esta omisión en la transposición signifique que en la ley española las exclusiones de responsabilidad producen el efecto impedir que puedan ejercitarse acciones de cesación contra los proveedores que reúnan los requisitos establecidos para beneficiarse de la exclusión de responsabilidad. De una parte, porque dicha conclusión sería directamente contraria a la directiva, y de otra parte, porque lo que se establece en los artículos 14 a 17 LSSI es que los intermediarios no podrán ser declarados responsables de los contenidos, cosa que nada tiene que ver con el hecho de que pueda o no dirigirse contra ellos una acción en la que lo que se solicita no es que se declare su responsabilidad, sino que se ordene el cese de la prestación del servicio respecto de un determinado contenido de carácter ilícito.[16]

Sorprende, por tanto, la conclusión a la que llegó el Auto de 10 de noviembre de 2004, por el que se denegaron las medidas cautelares de cesación solicitadas contra el proveedor de acceso y transmisión Bitmailer, S. L.[17] El auto llegaba a la conclusión de que la exclusión de responsabilidad establecida en el artículo 14 de la LSSI para los servicios de transmisión y de provisión de acceso comporta «la consecuencia indirecta de que no resulte legalmente posible atribuir a quienes prestan esa clase de servicios, fuera del deber general de colaboración con las autoridades que establece el art. 11 y al que más adelante haremos referencia, un deber propio y genuino de cesación o de retirada de contenidos aún en el supuesto de conocer el carácter ilícito de los mismos»,[18] y que en consecuencia no es posible estimar una acción de cesación contra tales prestadores, por más que dicha acción se halle prevista en disposiciones vigentes del ordenamiento, puesto que dichas disposiciones deben integrarse con las reglas de la LSSI, con el resultado de que el prestador que reúne los requisitos para gozar de la exclusión de responsabilidad prevista en el artículo 14 LSSI deja de tener legitimación pasiva para soportar acciones de cesación, precisamente en virtud de dicho artículo 14 LSSI.

El prestador de servicios de acceso en este caso concreto era la compañía Bitmailer, S. L. Dicho operador proporcionaba la conexión a Internet al sitio web weblisten.com.[19] Este sitio web desarrollaba una actividad de venta de música en línea que infringía los derechos de propiedad intelectual de los productores de fonogramas. Las compañías discográficas Emi, BMG, Universal y Sony habían obtenido en diversos procedimientos judiciales la declaración de que la actividad de este sitio web constituía, en relación con los fonogramas producidos por dichas compañías, una violación de sus derechos exclusivos de reproducción y de comunicación pública, así como un acto de competencia desleal. Los diversos procedimientos iniciados contra Weblisten S. A. habían ya ordenado a esta compañía el cese de su actividad infractora. Sin embargo, probablemente ante un lento o defectuoso

16. En este sentido se manifiestan también José MASSAGUER (enero-abril 2003). «La responsabilidad de los prestadores de servicios en línea por las infracciones al derecho de autor y los derechos conexos en el ámbito digital. El Tratado de la OMPI sobre Derecho de Autor (WTC) y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT)». *Revista de Propiedad Intelectual*. Núm. 13, pág: 11-48, esp. pág. 36; José Javier GONZÁLEZ DE ALAIZA CARDONA (2005). «Deberes y responsabilidades en materia de propiedad intelectual». En: Santiago CAVANILLAS MÚGICA (coord.). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, Comares, Granada. Pág. 226-256, esp. pág. 244. *Vid*. asimismo Juan José MARÍN LÓPEZ (2005). «La comercialización de la música a través de Internet y los derechos del productor de fonogramas: los casos "Weblisten" y "Bitmailer"». *Revista de la Facultad de Derecho de la Universidad de Granada*. Vol. 8, pág. 363-386.
17. Auto de 10 de noviembre de 2004, del Juzgado de lo Mercantil n. 2 de Madrid (ponente: Pedro María GÓMEZ SÁNCHEZ), publicado en el *Diario La Ley*, número 6186, miércoles, 9 de febrero de 2005, y disponible en las bases de datos de La Ley y de Aranzadi. En esta última base de datos se indica como fecha del Auto el día 3 de noviembre, mientras que en la base de datos de La Ley, la fecha es del 10 de noviembre. En todo caso se trata del mismo Auto.
18. Razonamiento Jurídico Tercero del Auto.
19. Bitmailer S. L. proporcionaba el servicio de acceso a la red a los servidores en que se alojaba el sitio www.weblisten.com. Bitmailer prestaba dicho servicio a Weblisten indirectamente, a través de la empresa Net Provider S. A., aunque las demandantes sugerían que tras el velo de la personalidad diferenciada existía identidad de substrato personal entre Net Provider S. A. y Weblisten S. A. Para un comentario global a las diversas sentencias recaídas en el caso Weblisten, puede verse Juan José MARÍN LÓPEZ (2005). «La comercialización de la música a través de Internet y los derechos del productor de fonogramas: los casos "Weblisten" y "Bitmailer"». *RFDUG*. Vol. 8, pág. 363-386; Fernando CARBAJO CASCÓN (2005-2006). «El caso "Weblisten" y sus implicaciones para el futuro de la gestión de los derechos de propiedad intelectual sobre los contenidos musicales en Internet». *ADI*. N.º 26, pág. 615-674.

cumplimiento de esta orden por parte de Weblisten, las compañías discográficas decidieron entablar una nueva acción, concretamente una acción de cesación, dirigida no contra Weblisten sino contra el proveedor que proporcionaba a Weblisten la conexión a Internet, Bitmailer S. L., con el objeto de que el juez ordenara a este último, que suspendiera la conexión a Internet de los equipos de Weblisten. Se solicitaba del juez que adoptara esta orden desde el principio del procedimiento como medida cautelar. Las demandantes argumentaban que el proveedor Bitmailer, S. L., al conectar a Internet los contenidos del sitio www.weblisten.com, debía considerarse cooperador respecto de la infracción de propiedad intelectual y del acto de competencia desleal, por lo que resultaría legitimado pasivamente para la correspondiente acción de cesación, en virtud de los artículos 139 de la Ley de Propiedad Intelectual y 18.2 y 20.1 de la Ley de Competencia Desleal. (Conviene notar que el auto es anterior a la modificación del Texto Refundido de la Ley de Propiedad Intelectual derivada de la transposición de las Directivas 2001/29/CE sobre derechos de autor y derechos afines en la sociedad de la información[20] y 2004/48/CE, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual.[21] Como consecuencia de la transposición de estas directivas al derecho español, el texto vigente de la Ley de Propiedad Intelectual recoge expresamente la posibilidad de adoptar medidas de cesación y otras medidas cautelares contra los intermediarios, a pesar de que los actos de éstos no constituyan en sí mismos infracción).[22]

El juez señaló que al tratarse de una actividad que se lleva a cabo por medio de Internet, la capacidad de soportar pasivamente cualquiera de las acciones de cesación previstas en los citados preceptos de la LPI y de la LCD, debe ser integrada mediante las disposiciones de la LSSI. El juez destaca que mientras que en los casos de *linking*, *hosting* y *caching*, se establece el requisito de retirar los contenidos al efecto de poder gozar de la exclusión de responsabilidad, no ocurre así en el caso de mera transmisión y provisión de acceso, donde se prevé, siguiendo lo dispuesto en la directiva, que el prestador del servicio goza de la exclusión de responsabilidad mientras no haya «originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos» (art. 14 LSSI). El juez considera que si el artículo 14 LSSI no ha previsto para estos prestadores una «obligación» de cesar en la prestación del servicio, hay que entender que dicho artículo ha venido a proteger al prestador frente al ejercicio de acciones de cesación previstas en el ordenamiento.

Como se ha dicho, esta conclusión no se compadece con el texto de la directiva, que, tras establecer la misma exclusión de responsabilidad que luego acogerá la LSSI, se cuida de destacar que la cobertura de responsabilidad no es óbice para mantener la legitimación pasiva ante acciones de cesación y remoción. Pero el problema principal, en mi opinión, es que el auto parte de una concepción errónea de las reglas de exclusión de responsabilidad de la LSSI. Dichas reglas contemplan determinadas actividades de intermediación y establecen que, en la medida en que la actividad desarrollada por el prestador se ciña a lo descrito en el supuesto de hecho, y cumpla con una serie de requisitos dirigidos a asegurar que estamos ante una función de intermediación puramente pasiva y neutra, dicho prestador no podrá ser declarado responsable de los contenidos intermediados en el caso de que éstos resulten ilícitos. Entre los requisitos para disfrutar de la exclusión de responsabilidad se halla (en el caso del *hosting* y del *linking*) el de retirar el material ilícito una vez que se ha tenido conocimiento efectivo de su ilicitud. Este último requisito no está dirigido tanto a asegurar el carácter neutro de la actividad de prestador, como a limitar los efectos de la exclusión de responsabilidad. En efecto, dicha exclusión, en el caso del *hosting* y del *linking*, exige no tener conocimiento de la ilicitud. De modo que el prestador queda a cubierto de toda posible responsabilidad mientras permanezca en dicha situación de desconocimiento. Una vez que haya obtenido el conocimiento efectivo, su continuación en la

20. La transposición de la directiva se ha llevado a cabo mediante la Ley 23/2006, de 7 de julio, por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril (BOE núm. 162 de 8 de julio).
21. La transposición de esta directiva se ha verificado por medio de la Ley 19/2006, de 5 de junio, por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios (BOE núm. 134, de 6 de junio).
22. *Cfr*. arts. 138, 139 y 141 de la Ley de Propiedad Intelectual.

intermediación de los contenidos ilícitos ya no se considera una función a la que pueda concederse de modo general una exclusión de responsabilidad.

Dicho de otro modo: los requisitos que se establecen en los artículos 14 a 17 LSSI no constituyen en sentido propio obligaciones o deberes que el legislador impone a los prestadores. Constituyen tan sólo elementos que permiten considerar la actividad como neutra o pasiva en relación con los contenidos intermediados, lo que posibilita conceder a dicha actividad una exclusión general de responsabilidad. En consecuencia, el hecho de que el prestador no satisfaga los requisitos previstos en dichas normas no constituye un incumplimiento de un deber legal. La única consecuencia de no cumplir con dichos requisitos es la imposibilidad de disfrutar de la exclusión de responsabilidad. El hecho de no poder invocar dicha exclusión tampoco significa que el prestador vaya a ser automáticamente responsable de los contenidos. Esto es así porque los artículos 14 a 17 no son normas de atribución de responsabilidad, sino de exclusión de responsabilidad. Que el prestador no puede valerse de dicha exclusión no significa necesariamente que se le pueda declarar responsable. Para esto último, es preciso que alguna norma del ordenamiento anude a la conducta de dicho prestador la consecuencia del deber legal de responder de los contenidos. Para que surja dicho deber, naturalmente, deberán concurrir todos los requisitos que esa norma de atribución de responsabilidad haya dispuesto para ello. En el caso de la responsabilidad civil, deberá considerarse tanto la negligencia como la existencia del daño, así como la relación de causalidad. En el caso de la responsabilidad penal, deberán concurrir todos los elementos necesarios para el nacimiento de la misma. No es posible interpretar *a contrario* las reglas de exclusión de responsabilidad. No son preceptos que imputen responsabilidad al prestador que no cumple los requisitos necesarios para la exclusión. Nótese que por ello es más correcto hablar de exclusión que de exención de responsabilidad, ya que este último término presupone que existe un deber legal previo de responder por los contenidos de terceros y que sólo gracias a una norma especial se exime de dicho deber al intermediario. En realidad, lo que la norma hace es garantizar que no se podrá declarar la responsabilidad del prestador, sin prejuzgar si su actividad es generadora de responsabilidad (civil, penal o administrativa) con arreglo a las normas que en nuestro ordenamiento atribuyen estos tipos de responsabilidad. Éste es el sentido de la directiva, que parte de la base de que las normas de atribución de responsabilidad son distintas en los diversos Estados Miembros.[23]

El auto que comentamos, considera, por el contrario, que los artículos 14 a 17 LSSI establecen una serie de obligaciones a cargo de los prestadores de servicios intermediarios, y que sancionan el incumplimiento de dichas obligaciones con la atribución de responsabilidad civil por los contenidos intermediados. Así es de ver en el discurso del juez:

> «Si una norma jurídica define consecuencias adversas –en este caso en términos de responsabilidad civil– para ciertas clases de personas cuando éstas realizan determinadas conductas (de acción o de omisión), esa norma está estableciendo al propio tiempo, de forma indirecta, específicas obligaciones (de abstención o de acción, respectivamente) cuyo cumplimiento incumbe a dichos sujetos. En otras palabras, si los arts. 14 y ss. de la Ley 34/2002 no imponen a los prestadores de servicios de intermediación explícitas obligaciones, pero en cambio les atribuyen responsabilidad civil cuando se abstienen, *vrg*., de retirar los contenidos que albergan en determinados supuestos, ello implica, en definitiva, que, concurriendo los supuestos legalmente previstos, la ley está imponiendo al prestador una obligación –propia y personal– de proceder a dicha retirada, obligación que, atendiendo a la cuádruple clasificación del art. 1089 del Código civil, no puede calificarse sino como de origen legal. En definitiva, lo único que late detrás de esa disquisición es una mera cuestión de técnica legislativa, donde no pueden advertirse diferencias sustanciales entre, por un lado, la hipotética opción del legislador de haber definido primero las obligaciones para pasar después a establecer las consecuencias de su incumplimiento y, por otro, la fórmula más abreviada –la que de hecho se ha adoptado por la referida ley– de determinar directamente las consecuencias (responsabilidad civil) que se anudan, bajo presupuestos definidos, a la ejecución o inejecución de conductas específicas. Consecuentemente, si de acuerdo con lo que acaba de razonarse podemos colegir que la Ley 34/2002 impone a los prestadores de servicios de intermediación, aunque sea mediante formulaciones de tipo indirecto, una concreta obligación de cesación (retirada de contenidos) en determinadas circunstancias, resulta obvio que dicha ley ha de cumplir una función integradora a la hora de definir los sujetos pasivos a quienes puedan llegar a incumbir las acciones de cesación reguladas de modo general en la Ley de Propiedad Intelectual y en la Ley de Competencia Desleal cuando los contenidos ilícitos vulneradores de estas leyes se ejecutan, transmiten y difunden a través de la Red.»

23. *Cfr*. a este respecto el considerando 9 de la Directiva sobre el Comercio Electrónico.

3. La discusión sobre el sentido del requisito de falta de «conocimiento efectivo»

La DCE establece en su artículo 14, como requisito para disfrutar de la exclusión de responsabilidad por alojamiento de materiales, que el prestador del servicio no tenga «conocimiento efectivo de que la actividad [*sic*] a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito».

La transposición al ordenamiento español se separa notablemente del texto comunitario al prescindir del requisito de carecer de conocimiento indiciario (conocimiento de hechos o circunstancias que revelen la ilicitud) que la directiva exige para quedar libre de responsabilidad civil. Y se separa también de lo dispuesto en la directiva al ofrecer una noción restrictiva de «conocimiento efectivo», que, interpretada en sentido estricto, desnaturaliza lo previsto por el legislador comunitario, ya que limita el concepto de conocimiento efectivo a un conocimiento formal derivado fundamentalmente de la existencia de una previa resolución que hubiera declarado la ilicitud del material.

Esta noción restrictiva es la que se sigue del artículo 16.1.II LSSI, donde se señala que «[s]e entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse». El mismo párrafo se reitera para la exclusión de responsabilidad por provisión de enlaces e instrumentos de búsqueda en el artículo 17.1.II LSSI.

Este texto plantea el problema de su interpretación. Si se interpreta en sentido «limitativo», sólo podrá apreciarse la concurrencia de conocimiento efectivo si se da alguno de los supuestos contemplados en dicho párrafo (previa resolución, acuerdos de notificación y retirada, o bien otros medios que en el futuro pueda fijar el legislador); mientras que si se interpreta en un sentido «no limitativo», será posible apreciar la concurrencia de tal conocimiento siempre que el mismo exista realmente y así se pruebe por cualquier medio admitido en derecho, con independencia de que se hayan verificado o no los supuestos de adquisición del conocimiento efectivo previstos en el párrafo que comentamos.

La jurisprudencia no ha sido uniforme en la interpretación de este párrafo de los artículos 16 y 17 LSSI. Algunas resoluciones, interpretando en sentido restrictivo este texto, han considerado que, al no haber existido una resolución judicial o administrativa previa que declarara la ilicitud del contenido, el intermediario carece del conocimiento efectivo previsto en la ley, y por tanto, conserva el beneficio de la exclusión de responsabilidad, con independencia del conocimiento real que pudiera tener de dichos contenidos y de su ilicitud. Otras resoluciones, por el contrario, parecen entender que no es necesaria la concurrencia de una previa resolución que declare la ilicitud, y por tanto que se puede adquirir el conocimiento efectivo por otros medios. En ningún caso, sin embargo, se ofrecen argumentos específicamente destinados a sostener una u otra interpretación. Veamos a continuación algunos ejemplos.

La primera resolución judicial que aplicó las normas de exclusión de responsabilidad de la LSSICE fue un auto de sobreseimiento provisional adoptado en unas diligencias previas por un delito de revelación de secretos contra el titular del sitio web ajoderse.com. Se trata del Auto de 7 de marzo de 2003 del Juzgado de Instrucción núm. 9 de Barcelona. El sitio web en cuestión consistía fundamentalmente en una relación de unas pocas decenas de enlaces a sitios externos, bajo el rótulo de «Colección de links de Seca Nagra». La temática común a la mayoría de materiales enlazados era información sobre cómo eludir la codificación de señales de televisión de pago, ya mediante la difusión de las claves, ya por otras vías. Era poco menos que obvio que el titular del sitio había llevado a cabo una tarea de selección de sitios web en atención a su temática. Sin embargo, el auto decidió sobreseer las diligencias entendiendo que el titular del sitio web carecía de conocimiento «efectivo», puesto que no se habían dado las circunstancias del artículo 17.1.II, esto es, no constaba que se hubiera dictado previamente una resolución que hubiera declarado la

ilicitud de los materiales enlazados. El auto señala en sus fundamentos jurídicos:

> «Que puede existir responsabilidad por la colección de hiperenlaces según el texto de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, que en su art. 17 establece la responsabilidad en que incurre un sitio web cuando sabiendo que un contenido es ilícito, se expone un enlace a una página declarada ilegal. Se precisaría el conocimiento efectivo por parte del proveedor de servicios de que la actividad o la información a la que remite el hiperenlace es ilícita. Pero aun cuando el prestador de servicios conozca la ilicitud de las páginas enlazadas, la Ley 34/2002 define lo que se entiende como conocimiento efectivo en el último párrafo de su art. 17.1: "Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse."
>
> »Por tanto, al no haberse aportado a la causa prueba alguna de la que deriven indicios de existir una resolución del tipo al que se refiere el citado último párrafo del art. 17.1 de la Ley 34/2002, ni que el imputado como prestador de servicios conociera tal resolución, no resulta debidamente justificada la perpetración del delito que dio motivo a la formación de esta causa, por lo que al amparo del art. 641.1 de la LECr en relación con lo establecido en el art. 789.5.1 o de dicho texto legal procede decretar el Sobreseimiento Provisional de la misma, sin perjuicio de su reapertura si se aportaran nuevos datos que pudieran constituir indicios de la perpetración del delito.»[24]

El auto rechaza, por tanto, la posibilidad de apreciar la existencia de conocimiento efectivo en el titular del sitio web obtenido por medios distintos de los previstos en el artículo 17.1.II, con independencia de la situación de conocimiento real que pueda tener el interesado, interpretando así el precepto en sentido restrictivo.[25]

Otro ejemplo, éste de la jurisdicción civil, puede resultar ilustrativo de la interpretación cerrada de la noción de conocimiento efectivo. Se trata de la sentencia de la AP de Madrid (secc. 14.ª), de 20 de diciembre de 2005.

En el sitio web www.aprendizmason.org se publicaron determinados artículos atentatorios contra el honor de la persona que había desempeñado anteriormente el cargo de gran maestro de la Gran Logia de España. Este sitio web se hallaba alojado en el conocido portal iEspaña, que presta servicios de alojamiento web. Los datos de identificación del titular del sitio web eran falsos, por lo que se desconocía su verdadera identidad. El agraviado requirió por conducto notarial al proveedor iEspaña poniéndole en conocimiento de la ilicitud de los contenidos publicados en el mencionado sitio web, identificando concretamente los artículos y exigiendo su retirada, requiriéndole además para que le indicara la verdadera identidad del titular del sitio web al efecto de poder ejercitar las acciones oportunas. El proveedor iEspaña no procedió a la retirada de dichos contenidos y se limitó a advertir al propietario de la página, a través de un comunicado en la propia página web, que había recibido el requerimiento notarial que identificaba contenidos que podían ser atentatorios contra el honor. El ofendido presentó demanda por vulneración del derecho al honor contra iEspaña alegando, en lo que aquí interesa, que dicho prestador de servicios era responsable, solidariamente con el desconocido autor de los contenidos, de haber permitido que los artículos permanecieran en el sitio web, aun después de haber recibido el requerimiento notarial y por tanto tener constancia de su ilicitud, y de permitir que se publicaran en el mismo nuevos artículos difamatorios. En su demanda invocaba expresamente el artículo 16 de la LSSI y alegaba negligencia por parte de la demandada. Ésta opuso que carecía de legitimación pasiva, ya que no podía retirar los artículos escritos por terceros por resultar contrario al derecho fundamental a la libertad de expresión; que aun sin estar obligada a ello comunicó la queja al autor de la página; y que mientras no recayera una resolución judicial que determinara que los artículos de opinión publicados eran ilícitos y ordenara su retirada, no se le podía exigir responsabilidad, en aplicación del artículo 16 LSSI. La sentencia de 5 de mayo de 2004, del Juzgado de Primera Instancia núm. 3 de Alcobendas, determinó que los contenidos publicados efectivamente lesionaban la dignidad del demandante y menoscababan su prestigio personal y profesional. El autor de los mismos, sin embargo, era desconocido. El registro del nombre de dominio lo había gestionado el propio proveedor iEspaña ante un registrador de nombres de domino francés el 8 de abril de 2002, a favor del cliente que se había identificado con datos falsos. Dicho registro caducó un año después, y

24. El texto completo del auto puede consultarse en: http://www.bufetalmeida.com/76/ajodersecom-primera-interpretacion-judicial-de-la-LSSI.html [fecha consulta. 10/03/2007].
25. Por otra parte, el auto parece considerar que el incumplimiento de las condiciones establecidas en el artículo 17 LSSI para gozar de la exclusión, genera automáticamente responsabilidad, en virtud de una suerte de interpretación *a contrario* del precepto que ya hemos tenido ocasión de criticar más arriba.

a la fecha de la sentencia el sitio web ya no se hallaba alojado en el portal iEspaña. La sentencia de instancia desestimó la demanda considerando que la demandada quedaba exenta de responsabilidad en virtud del artículo 16 LSSI, ya que no había existido una previa declaración por el órgano competente de la ilicitud del contenido de la página web ordenando su retirada o imposibilitar el acceso a la misma, ni de la existencia de lesión del derecho al honor del actor. La sentencia razonaba además que no existía espacio alguno de impunidad, porque el ofendido podía haber acudido a lo dispuesto en el artículo 8 LSSI.

El demandante recurrió en apelación, y la sentencia de 20 de diciembre de 2005, de la Audiencia Provincial de Madrid (Sección 14) confirmó la absolución de la demandada. De acuerdo con esta sentencia,

> «A los prestadores de servicios de alojamiento o almacenamiento de datos, al igual que a los que faciliten enlaces a contenidos o instrumentos de búsqueda, sólo se les podrá hacer responsables en dos supuestos: cuando tengan conocimiento efectivo de que la información almacenada o que es objeto de enlace o búsqueda, es ilícita o de que puede lesionar bienes o derechos de un tercero susceptibles de indemnización y cuando, teniendo este conocimiento, no actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos; entendiéndose que el servidor conoce la ilicitud de esa información a la que presta un servicio determinado "cuando el órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse", como dice el artículo 16; el legislador español, con el fin de no menoscabar el ejercicio del derecho a la libertad de expresión y otros valores ha optado por la no obligación de fiscalizar los contenidos por parte de los prestadores de servicios, si bien les impone un deber de diligencia, concretado, aparte de lo establecido en el artículo 16, en el artículo 11, que establece una serie de obligaciones en relación con los contenidos, y de colaboración con las autoridades públicas para localizar e imputar responsabilidad a los autores de actividades o contenidos ilícitos que se difundan por la Red o para impedir que éstos se sigan divulgando.
>
> »(...) Siendo evidente, y así viene a aceptarlo el actor en su recurso de apelación, que la responsabilidad de la demandada no puede surgir en aplicación del artículo 16 de la Ley 34/02, porque no había tenido conocimiento efectivo, *en el sentido dado por el precepto*, de que los artículos de opinión lesionaran el derecho al honor del actor y no venía obligada a retirar o imposibilitar el acceso a los artículos, so pena de convertirse en órgano censor vulnerador del contrato celebrado con el cliente y, de resolverse finalmente que no había existido vulneración del derecho al honor, en trasgresora del derecho a la libertad de expresión del referido cliente, e, incluso, había advertido al propietario de la página, a través de un comunicado en la propia página web, que había recibido una carta notarial por la publicación de "documentos" posiblemente atentatorios contra el honor del actor, (...)».[26]

A la vista de estos razonamientos es claro que la sentencia lleva a cabo una interpretación cerrada o limitativa del artículo 16.1.II. Por otra parte, al igual que hiciera la sentencia de instancia, la Audiencia afirma que no hay un espacio de impunidad, porque el actor bien podía haber actuado los procedimientos a que se refiere el artículo 8 de la LSSI cuando tuvo conocimiento de la publicación del primer artículo. Parece, pues, que el tribunal se refiere a que el agraviado tenía la posibilidad de instar al órgano competente, en este caso judicial, para que ordenara la interrupción del servicio o la retirada de los contenidos por vulnerar principios recogidos en el citado artículo 8.

Es interesante, por lo demás, destacar que la sentencia recuerda que el Tribunal Constitucional ha declarado que el artículo 65.2 de la Ley 14/1966 de 18 de marzo, de Prensa e Imprenta no es incompatible con la libertad de expresión consagrada en el artículo 20.1 de la Constitución, porque la responsabilidad civil solidaria, entre otros, del director del medio periodístico y de la empresa editora se justifica en la culpa *in eligendo* o *in vigilando* del editor o del director, dado que ninguno de ellos son ajenos al contenido de la información y opinión que el periódico difunda, pues el director puede vetar cualquier original, y a la empresa editora le corresponde la libre designación del director.[27] Añade sin embargo la sentencia de la Audiencia:

> «Ello no es equiparable al prestador de servicios y por ello mismo la Ley 34/02 opta por exonerarles de responsabilidad, con las salvedades aquí inaplicables, ya que es imposible controlar el enorme volumen de información que se introduce en los ISP y el prestador de servicios no puede equipararse a un editor porque es un mero distribuidor de la información; la equiparación que procede es editor-creador de la página web (aquí el cliente de la demandada); no la de editor-propietario del ordenador donde se aloja la información o editor-servidor. La proveedora de servicios demandada carecía de capacidad de decisión respecto de los contenidos de la página web creada y es extrema la dificultad para comprobar si los datos proporcionados por los clientes al contratar por contrato electrónico son ciertos o no lo son, de modo que no concurrían los requisitos exigidos por el artículo 1902 del Código Civil cuya aplicación pretende el apelante, ni resultaba aplicable la analogía.»[28]

26. Sentencia de 20 de diciembre de 2005 de la Audiencia Provincial de Madrid (Sección 14), recurso de apelación n.º 229/2005, ponente: Amparo Camazón Linacero. Fundamentos Jurídicos segundo y tercero. El énfasis es nuestro.
27. *Cfr*. SSTC 171/1990, FJ 3.º y 172/1990, FJ 7.º.
28. Sentencia de 20 de diciembre de 2005 de la Audiencia Provincial de Madrid (Sección 14), recurso de apelación n.º 229/2005, ponente: Amparo Camazón Linacero. FJ 4.º.

Junto a estas interpretaciones de carácter cerrado, que entienden el texto de los artículos 16.1.II y 17.1.II como una definición de conocimiento efectivo, y consideran por tanto que éste sólo puede existir si se ha obtenido por las vías contempladas en dicho texto, se han dictado también resoluciones judiciales que admiten la posibilidad de apreciar la concurrencia de conocimiento efectivo sin que se hayan verificado las circunstancias del citado texto legal. En este sentido podemos citar dos casos.

El primero es el de la SGAE contra la Asociación de Internautas. Se trata del procedimiento resuelto en Sentencia de 15 de junio de 2005, del Juzgado de 1.ª Instancia número 42 de Madrid, confirmada en apelación por Sentencia de 6 de febrero de 2006 de la Sección 19.ª de la Audiencia Provincial de Madrid, en la actualidad recurrida en casación ante el Tribunal Supremo y pendiente de resolución.

La Sociedad General de Autores y Editores y su presidente D. Eduardo Bautista formularon demanda de juicio ordinario contra la Asociación de Internautas por determinadas expresiones atentatorias contra el derecho al honor de los demandantes contenidas en una página alojada en los servidores de la Asociación. Los contenidos de dicha página web eran obra de la «Plataforma de Coordinación de Movilizaciones contra la SGAE». La página, ubicada en http://antisgae/internautas.org, era un *mirror* de otro sitio web, www.putasgae.org, perteneciente a aquella plataforma y no alojado en los servidores de la asociación. Se daba la circunstancia de que el nombre de dominio «putasgae.org» figuraba registrado a nombre de la asociación; sin embargo, ésta alegó que el verdadero titular era la mencionada plataforma, que había indicado un nombre falso en el registro del dominio, y en cuanto la asociación tuvo conocimiento de ello, conminó a la plataforma a rectificar ese dato. Aunque la asociación alegó su carácter de prestador de servicios de alojamiento, la sentencia de instancia argumentó del siguiente modo:

> «Lo cierto es que la demandada afirma, y ello sería en cualquier caso innegable que ha servido de "mirror" de los contenidos elaborados por la plataforma y que ofreció albergue a dicha plataforma para que publicara sus contenidos. Es indiferente pues que la demandada tuviera el dominio de la página a la que pertenece la dirección de Internet www.putasgae.org o que se limitara a una labor de prestación de servicios. En cualquiera de los casos habría de responder de los contenidos antes dichos pues si presta el servicio a la plataforma es responsable también de los contenidos de esta pues por el simple hecho de ser el prestador del servicio que presta el dominio o subdominio, como bien subrayó el Ministerio Fiscal adquiriría responsabilidad sino por dolo sí por negligencia al permitir utilizar en su dominio manifestaciones injuriosas pues si bien el representante legal de la asociación ha declarado que él no ejerce control sobre los contenidos, lo cierto es que el que presta un servicio ha de controlar lo que se publica en sus páginas pues si presta su dominio para que se publiquen unos contenidos también puede y debe impedir que se publiquen si son ilícitos, al menos civilmente como ocurre en este caso.»[29]

La sentencia de instancia no hace referencia alguna a la LSSI, y entre otros pronunciamientos condena a la Asociación de Internautas a cesar en la perturbación en el derecho al honor de los actores, a suprimir las expresiones atentatorias contra el mismo, a indemnizar a cada uno de los actores con 18.000 euros, y a publicar la sentencia firme que recaiga, además de al pago de las costas.

La asociación recurrió en apelación y alegó entre otros argumentos infracción de la LSSI, norma que ya había invocado en la primera instancia. La sentencia de apelación afirma que la LSSI no excluye la aplicación de la otras normas, como la Ley Orgánica 1/1982, de 5 de Mayo, de Protección Civil del Derecho al Honor, la Intimidad Personal y Familiar y la Propia Imagen, y concluye que:

> «la responsabilidad por las intromisiones en el honor, intimidad y propia imagen, no se ha de derivar sólo al autor de la información, sino también al intermediario, que soluciona los contenidos y los introduce en la red, poniendo a disposición de los usuarios una determinada información, ya sea en una página web, una base de datos o una lista de distribución, *con la matización* de que procede entender responsable al creador y el editor de la información, y a los proveedores de acceso y servicios sobre la base del efectivo conocimiento y la posibilidad técnica de control de la información».[30]

Hecha esta afirmación, la sentencia vuelve a la cuestión de la discusión sobre la titularidad del nombre de dominio putasgae.org. Señala que el hecho de aparecer la asociación como registrante de dicho dominio,

> «cuando menos le obliga a articular prueba para destruir esa más [*sic*] presunción de titularidad, prueba que no articula, desde lo precedente y valorando lo que en la contestación a la demanda se indica en cuanto a que la [demandada] mantiene postura encontrada con la demandante en la materia referida a la remuneración compensatoria o canon por copia privada en los soportes digitales, diferencias que mantiene de forma activa, llegamos la plena convicción de la responsabilidad de la demandada en la denominación putasgae y en los contenidos a los que la demanda se refiere como atentatorios al honor de los demandantes».[31]

29. Sentencia de 15 de junio de 2005, del Juzgado de 1.ª Instancia número 42 de Madrid. Fundamento Jurídico 5.º.
30. Sentencia de 6 de febrero de 2006 de la Sección 19.ª de la Audiencia Provincial de Madrid (Ponente: Nicolás Díaz Méndez). Fundamento Jurídico 7.º. El énfasis es nuestro.
31. *Id*., Fundamento Jurídico 7.º.

Así, la sentencia parece llegar a la conclusión de que la demandada tenía conocimiento efectivo de los contenidos difamatorios, o incluso que realmente era autora o coautora de los mismos o bien que los hace propios al decidir darles alojamiento en su servidor. En el fundamento jurídico noveno la sentencia vuelve sobre esta idea indicando,

> «que las expresiones califican por sí ese carácter atentatorio al honor, sin que puedan venir amparadas en la tesis del reportaje neutral, y desde lo antes considerado en relación con la titularidad del dominio también indicado, y de lo expresado en orden a la responsabilidad también referida, pues se rompe la neutralidad cuando son varios medios los que difunden información o manifiestan expresiones con plena autonomía, sin que haya de demandarse a todos, máxime como [*sic*] en supuestos como el de autos en que *se procede a recopilación para hacer propios los contenidos*;»[32]

En ningún momento la sentencia hace un análisis explicito sobre la concurrencia de los requisitos del artículo 16 LSSI. Simplemente, como hemos visto, indica que es necesario para la responsabilidad del intermediario que exista «efectivo conocimiento y posibilidad técnica de control», lo que parece que da por hecho al entender que la demandada ha hecho propios los contenidos.[33]

Un segundo ejemplo que parece aceptar la línea de interpretación no limitativa de la noción de conocimiento efectivo es el Auto de la AP de Cáceres (secc. 2.ª), de 30 de octubre de 2006. El caso se refiere a la publicación de manifestaciones injuriosas en un foro de Internet. Se imputa al titular y administrador del foro la posible comisión de una o varias infracciones penales. El auto de la Audiencia no enjuicia el fondo del asunto, sino que resuelve la apelación presentada contra la desestimación de un recurso de reforma que pedía la nulidad del auto de 16 de marzo de 2006, dictado por el Juzgado de Instrucción n.º 3 de Plasencia. La Audiencia confirma la desestimación recurrida y señala que en ese momento procesal se trata simplemente de comprobar si existen indicios racionales de la comisión de dichas infracciones penales. En lo que se refiere a la responsabilidad por las injurias, el tribunal parece admitir que el administrador pueda ser responsable en aplicación del artículo 30 del Código penal, como consecuencia del sistema de responsabilidad «en cascada». Advierte también que dicha responsabilidad podría quedar excluida en virtud del artículo 16 de la LSSI. En el caso concreto, el administrador procedió al borrado de los mensajes injuriosos, lo que a juicio de la Audiencia podría responder a que tenía conocimiento de su ilicitud, si bien también podría constituir el cumplimiento de la condición de retirar el material que se exige para conceder la exclusión de responsabilidad. El fundamento jurídico tercero del auto se expresa en estos términos:

> «Tercero. Se imputa al recurrente la comisión de un delito contra el honor del que sería autor al amparo de la regla de responsabilidad escalonada en relación con los delitos cometidos utilizando medios o soportes de difusión mecánicos del artículo 30 del Código penal, al ser el titular y administrador del foro en el que se vertieron las expresiones ofensivas denunciadas.
>
> »El artículo 13.1 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico establece que "los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley", por lo que las reglas del artículo 30 del Código penal resultan en principio de aplicación.
>
> »No obstante, esa regla también debe entenderse limitada o matizada por lo expuesto en el artículo 16.1 de la Ley especial, que señala que "Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o, b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos."
>
> »Si el imputado conocía o no el contenido de aquellos mensajes es una cuestión que no puede ser objeto de una decisión de fondo en el trámite que ahora nos ocupa, ya que exigiría una verdadera valoración de pruebas propia del juicio. Basta, como decimos, con la existencia de elementos indiciarios para la validez de la resolución impugnada, y el hecho de que los mensajes originales o iniciales fueran borrados incluso antes de la incoación de las diligencias penales puede ser compatible con el hecho de que el imputado conociera su contenido (aunque también con la diligencia a que se refiere el apartado "b" citado). Obviamente estos indicios no bastarán para su condena y habrán de ser corroborados por pruebas susceptibles de destruir la presunción de inocencia que constitucionalmente se le reconoce.»[34]

32. *Id*., Fundamento Jurídico 9.º. El subrayado es nuestro.
33. La sentencia, como indicábamos, se halla recurrida en casación, por lo que habrá que esperar a conocer la resolución que dicte el Tribunal Supremo, que constituirá una buena ocasión para sentar jurisprudencia acerca de la interpretación que deba darse al requisito del conocimiento efectivo para gozar de la exclusión de responsabilidad.
34. Auto de 30 de octubre de 2006, de la Audiencia Provincial de Cáceres, Sección 2.ª, recurso 353/2006, ponente: Valentín Pérez Aparicio.

El auto parece, pues, aceptar una interpretación no limitativa de la noción de conocimiento efectivo, por cuanto indica que cabe la posibilidad de que el imputado hubiera tenido dicho conocimiento a pesar de que no consta que hubiera una previa declaración de la ilicitud dictada por órgano competente. Parece dejar abierto también el tema de si la retirada fue o no diligente. El caso tiene un elemento añadido que lo complica un poco, y es que se imputa también al administrador un delito de desobediencia porque el agente de la Guardia Civil le ordenó que en tanto continuara la investigación no modificara ni alterara ninguno de los mensajes del foro, a pesar de lo cual el administrador imputado eliminó el foro tres días después. Se le imputa además un delito de encubrimiento, puesto que al suprimir el foro, eliminó también toda posibilidad de conocer las direcciones IP desde las que se enviaron los mensajes, haciendo así imposible la identificación de los autores directos, respecto de los cuales las actuaciones penales se sobreseyeron.

A la vista de los casos expuestos, resulta clara la discrepancia entre distintas resoluciones judiciales a la hora de interpretar qué debe entenderse por conocimiento efectivo a los efectos de la aplicación de la exclusión de responsabilidad prevista en los artículos 16 y 17 LSSI.[35] No resulta fácil determinar qué opción interpretativa es la más correcta. De hecho, ambas lecturas presentan inconvenientes.

Una interpretación abierta o no limitativa plantea la dificultad de la literalidad del texto legal, aunque no se trata de una dificultad insalvable, puesto que cabe interpretar gramaticalmente el texto como una serie de presunciones

35. Hallándose este trabajo en fase de pruebas de edición, se ha dictado una nueva sentencia a la que es obligado hacer referencia brevemente, dejando para una futura ocasión un análisis más detenido.
Se trata de la sentencia núm. 184/2007, de 13 de septiembre de 2007, del Juzgado de Primera Instancia núm. 44 de Madrid. El objeto del conflicto en este caso son determinados contenidos del foro titulado «El Rey del Pollo Frito. Ramoncín», del sitio web alasbarricadas.org, que atentan contra el honor del demandante (Ramoncín). El cantante demandó al titular del sitio, solicitando que ciertas expresiones y fotografía presentes en el mismo se declararan intromisiones ilegítimas en su derecho al honor, se ordenara el cese de la perturbación suprimiendo tales contenidos, y se le condenara a la publicación a su costa de la sentencia y al abono de una indemnización de 6.000 euros. La sentencia estima íntegramente las peticiones de la demanda, incluida la condena en costas.
Conviene indicar que el sitio web cumplía sólo parcialmente con las obligaciones de identificación del art. 10 LSSI, puesto que si bien ponía a disposición de los usuarios una dirección de correo electrónico para contactar sobre cualquier cuestión relacionada con el mismo (info@alasbarricadas.org), no indicaba la identidad del titular del sitio, ni tampoco su domicilio físico. Dicha identidad, sin embargo, podía averiguarse fácilmente en los datos del registro del nombre de dominio, en la base de datos pública Whois. Allí constaba también su domicilio al tiempo que el registro del nombre, aunque por haber cambiado posteriormente de domicilio, este dato ya no resultaba útil como tampoco los hechos objeto de la demanda. El interés de reseñar estos particulares reside en que la argumentación de la sentencia para declarar la responsabilidad del demandado se basa en una lectura conjunta de los arts. 16 y 10 LSSI, como veremos a continuación. Indiquemos antes que ambas partes consideran aplicable la LSSI, admitiendo pacíficamente que el sitio web tiene el carácter de prestador de servicios de la sociedad de la información (no se discute, por tanto, si su actividad es o no de naturaleza económica). Ambas partes admiten también que se trata de contenidos elaborados por terceros, lo que implica que resulte de aplicación el art. 16 LSSI.
La sentencia, como indicábamos, considera que el art. 16 debe ponerse en relación con el art. 10, en el sentido de que las obligaciones de identificación previstas en este artículo deben considerarse como parte de la diligencia exigible para poder disfrutar de la exclusión de responsabilidad prevista en el art. 16. Argumenta la sentencia que si no constan los datos de identificación, no es posible que el ofendido ponga en conocimiento del demandado la presencia de los contenidos injuriosos. (Subyace en este discurso la idea de que la comunicación del ofendido al titular del sitio web sería suficiente para que éste obtuviera el conocimiento efectivo, esto es, una interpretación no limitativa del art. 16.1.II.)
La discusión sobre si podría o no beneficiarse plenamente de la exclusión de responsabilidad un prestador de servicios que pusiera obstáculos a la obtención del conocimiento efectivo, impidiendo incluso la efectividad de los medios de obtención de dicho conocimiento previstos en el art. 16.1.II, me parece digna de atención y merecedora de un análisis más profundo del que es posible hacer en esta nota. Sin embargo, no me parece aceptable como criterio de decisión en el caso que nos ocupa, ya que si bien no constaban todos los datos de identificación, sí estaba a disposición del público una dirección de correo electrónico que permitía una comunicación directa con el titular del sitio. En un intento de salvar este escollo, la sentencia argumenta que el demandado tenía que haber probado en el juicio que dicha dirección era un medio de contacto eficaz: «Tampoco consta que la dirección de correo electrónico aportada fuese efectiva para contactar con él, limitándose genéricamente a alegar que es el medio habitual de contacto, pero no aportando prueba al efecto, como le compete una vez verificada la lesión de un derecho fundamental. Así, al invertirse la carga de la prueba bastaría con el que el demandado hubiese justificado mínimamente que se podía acceder a él con facilidad y de modo efectivo y que eran eficaces los medios que ponía a disposición de los usuarios para poder a su vez dar cumplimiento a su deber de diligencia, mediante prueba pericial o testifical objetiva» (*Cfr.* FJ 5). Esto parece un exceso desde todos los puntos de vista, puesto que la existencia de la dirección de contacto es admitida por el actor, que en ningún momento (por lo menos no en la demanda) objeta que dicha dirección no funcionara correctamente. No procede por tanto, reprochar al demandado no haber probado algo que el demandante no puso en cuestión. Por lo demás, la sentencia se extralimita de nuevo al añadir reproches de supuesta falta de diligencia del demandado que claramente van más allá de la diligencia suficiente para gozar de la exclusión de responsabilidad de acuerdo con el artículo 16, concretamente al indicar que el demandado «tampoco acredita o justifica la imposibilidad de contar con un moderador u otros filtros o que los contenidos se actualicen a diario o semanalmente, o las características de su sistema o aplicación informática de modo que se evite prolongar en el tiempo contenidos ilícitos o difamatorios».

legales de concurrencia de conocimiento efectivo, que no impiden apreciarlo en situaciones distintas. Por otra parte, plantea el inconveniente de que la situación resultante pueda ser excesivamente gravosa para los operadores en términos de riesgo de ser declarados responsables, así como un posible efecto adverso para la libertad de expresión.

Por su parte, una interpretación estricta o limitativa ofrece la seria dificultad de resultar contraria a la directiva, puesto que concede la exención a supuestos en que el titular tiene verdadero conocimiento de la ilicitud de los contenidos alojados. Mientras que la directiva dispone que la exclusión es inaplicable en todos los casos en que concurra conocimiento efectivo, la LSSI, interpretada en sentido limitativo, estaría estableciendo que mientras el conocimiento no se haya obtenido por las vías contempladas en el artículo 16.1.II, el hecho de tener conocimiento efectivo no será obstáculo para disfrutar de la exclusión de responsabilidad. Por lo demás, la tesis limitativa plantea el inconveniente de originar una inmunidad casi absoluta y convertir a menudo en ilusoria la posibilidad de obtener la reparación económica del perjuicio sufrido.

Desde mi punto de vista, la necesidad de interpretar la ley española de conformidad con la directiva apoya la conclusión de que el artículo 16.1.II debe leerse en un sentido no limitativo, conclusión que por coherencia interna debe extenderse también al artículo 17.1.II. Debe tenerse presente, sin embargo, que el mero conocimiento material de la presencia de determinados contenidos no significa necesariamente «conocimiento efectivo de la ilicitud», cosa que probablemente sólo deba apreciarse en los casos en que la ilicitud resulte obvia. Y por otra parte, es preciso tener en cuenta que el hecho de que el prestador tenga conocimiento efectivo y no pueda beneficiarse de la exclusión de responsabilidad, no implica, como indicábamos más arriba, que se convierta necesariamente en responsable de los contenidos, sino que la atribución de responsabilidad dependerá de lo que establezcan las normas generales y especiales de nuestro ordenamiento que rigen la imputación de responsabilidad.

En cualquier caso, si el Tribunal de Justicia de las Comunidades Europeas tiene ocasión de pronunciarse sobre las cuestiones prejudiciales planteadas por la recurrente y por el Ministerio Fiscal en el seno del procedimiento que enfrenta a la Sgae con la Asociación de internautas, podremos contar un sólido criterio para unificar la interpretación judicial en este campo en relación con la actividad de *hosting*, interpretación que probablemente se extenderá también al caso de la provisión de enlaces e instrumentos de búsqueda, a pesar de que la directiva no contempla, de momento, una exclusión de responsabilidad para estos supuestos.

Cita recomendada

PEGUERA, Miquel (2007). «"Sólo sé que no sé nada (efectivamente)": la apreciación del conocimiento efectivo y otros problemas en la aplicación judicial de la LSSI». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

<http://www.uoc.edu/idp/5/dt/esp/peguera.pdf>

ISSN 1699-8154

Sobre el autor

Miquel Peguera Poch

mpeguera@uoc.edu

Doctor en Derecho, profesor de Derecho mercantil y de Derecho y nuevas tecnologías en la UOC. Entre otras publicaciones, es autor de la monografía *La exclusión de responsabilidad de los intermediarios en Internet* (Comares, 2007). En la actualidad, es *visiting scholar* en la Columbia University School of Law.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

Perspectivas del derecho a la autodeterminación informativa

Pablo Lucas Murillo de la Cueva

Fecha de presentación: mayo 2007
Fecha de aceptación: junio 2007
Fecha de publicación: septiembre 2007

Resumen

La situación en que se halla el ordenamiento jurídico español en materia de protección de datos es en cierto modo contradictoria, ya que existe un reconocimiento del carácter fundamental del derecho a la protección de datos y un marco jurídico que lo desarrolla, sin embargo, las regulaciones sectoriales de este derecho son insuficientes.

En el ámbito público, existe una normativa que tiene implicaciones directas con el tratamiento de datos de carácter personal (DCP), alguna en fase de aprobación, que en ocasiones únicamente se remiten a la LOPD, y en otras es un tanto contradictoria con dicha ley orgánica. En cualquier caso, la AEPD y los tribunales deberán ser especialmente exigentes en su aplicación, a fin de proteger no sólo el derecho a la autodeterminación informativa, sino más allá, la propia libertad de las personas.

El sector privado requiere de una mayor atención, ya que no se halla sujeto a condicionamientos institucionales y los DCP constituyen un bien cada vez más valioso sin que el ciudadano sea siempre consciente de ello. En consecuencia, la información, formación y uso de códigos tipo son cada vez más necesarios.

En definitiva, nos hallamos en el comienzo de una nueva etapa. Hay que abordar la defensa del derecho a la protección de DCP con los medios jurídicos de que se dispone y no parece suficiente ni adecuado dejar simplemente a la iniciativa privada la defensa del derecho fundamental a la protección de DCP. La solución adecuada para garantizar este derecho es tanto la intervención pública como la actuación privada, dirigiendo e impulsando la primera a la segunda Se precisan regulaciones acordadas internacionalmente que velen por una actuación coordinada en defensa del derecho a la autodeterminación informativa.

Palabras clave

autodeterminación informativa, datos de carácter personal, códigos tipo, intervención pública, autorregulación

Tema

Protección de datos

Perspectives on the right to informative self-determination

Abstract

The current situation of the Spanish legal system as regards data protection is, to a certain degree, contradictory. The fundamental right to data protection is acknowledged and a legal framework exists for its development, but the sectorial regulations covering this right are insufficient.

Within the public ambit, regulations exist – others are awaiting approval – that have direct implications for the processing of personal data (PD): some are only remitted to the Organic Law on Data Protection and others are somewhat contradictory to this Law. Whatever the case, the AEPD (Spanish Data Protection Agency) and the Courts will have to be especially rigorous in the application of this Law in order to protect not only the right to informative self-determination, but personal freedom itself. The private sector requires greater attention as it is not subject to institutional conditions, and citizens are not always aware of the fact that PD constitutes an increasingly valuable asset. Consequently, information, training and use of model codes become increasingly necessary.

In short, we are at the advent of a new era. We must address the defence of our right to PD protection by using the existing legal resources, and it seems neither sufficient nor appropriate to leave the defence of our fundamental right to PD protection solely to private initiative. The adequate solution for ensuring this right encompasses public intervention and private actions, directing and driving the former towards the latter. It is vital that we have internationally-agreed regulations that ensure a coordinated action in defence of our right to informative self-determination.

Keywords

informative self-determination, personal data, model codes, public intervention, self-regulation

Topic

Data protection

1. El actual estado de las cosas

El derecho a la autodeterminación informativa, objeto de esta sesión, ha sido reconocido, bajo la denominación de derecho a la protección de datos de carácter personal, en la Carta de los Derechos Fundamentales de la Unión Europea, figura, por tanto, incluido en el Tratado por el que se establece una Constitución para Europa, y se ocupan de garantizarlo el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de las Comunidades Europeas, cada uno en su respectivo ámbito de actuación. Varias sentencias de uno y otro se han pronunciado sobre él.

Por lo que se refiere al ordenamiento español, además de la proyección que tienen en su seno los textos mencionados y la jurisprudencia de esas instancias jurisdiccionales, sucede que ha sido reconocido como derecho fundamental por el Tribunal Constitucional (STC 292/2000) y, de ese modo, preside, da sentido y unifica una normativa cada vez más amplia, establecida a partir de 1992, primero por la Ley Orgánica 5/1992 (LORTAD) y, después, por la Ley Orgánica 15/1999 (LOPD). De acuerdo con lo previsto por esa legislación, desde 1994 contamos con la Agencia Española de Protección de Datos, institución independiente, encargada de velar por su observancia, que desarrolla una intensa labor de defensa especializada del derecho a la autodeterminación informativa, tarea en la que la acompañan, si bien solamente respecto de los ficheros y tratamientos de los órganos autonómicos y de las entidades locales correspondientes, otras agencias de ámbito territorial, hasta ahora, la madrileña, la catalana y la vasca.

A su vez, las normas vigentes son aplicadas por los tribunales ordinarios, que también controlan la actuación de las agencias mencionadas, así como las de los restantes poderes públicos. Y, con sus sentencias, van despejando algunos puntos oscuros de la legislación vigente en la materia y están sentando una interpretación que se caracteriza por orientarse, en general, a dotar de la mayor efectividad a este derecho.

Por tanto, el escenario que tenemos a la vista puede verse como el punto de llegada o la meta a la que apuntaban las iniciativas que, desde mediados de los años ochenta, reclamaban la protección frente al avance tecnológico, y muy particularmente frente al uso de la informática (Lucas Murillo de la Cueva, 1990). En efecto, esa defensa se ha configurado como el objeto de un nuevo derecho fundamental que ha cobrado carta de naturaleza en el marco de la Convención Europea para la Salvaguarda de los Derechos Humanos, en el ordenamiento comunitario y en el ordenamiento constitucional español. Además, si reparamos en el texto del Tratado por el que se establece una Constitución para Europa, veremos que no sólo reconoce como fundamental el derecho a la protección de datos de carácter personal, algo que ya hacía la Carta de Niza del 2000. Da un paso adicional e incluye su respeto entre los elementos de la vida democrática de la Unión Europea, dotándole también de este modo de una dimensión objetiva específica que refuerza su significación.

Una vez sentado lo anterior, ayudará a situar mejor lo que sigue recordar sumariamente en qué consiste este derecho.

Bastará para ello con tener presente que la protección de datos de carácter personal es un derecho fundamental autónomo que subyace al artículo 18.4 de la Constitución y tiene por objeto principal poner en mano de los individuos todos los medios jurídicos para controlar el uso por terceros de sus datos personales. Del mismo modo que uno de los sentidos de la palabra autodeterminación es el que apunta al ejercicio por cada uno de la propia libertad, ese término con el calificativo «informativa» indica definición o control por el afectado de la información que le concierne.

El control que nos ofrece este derecho fundamental descansa en dos elementos principales. El primero es el del consentimiento del afectado como condición de licitud de las actividades de captación y utilización de datos personales por terceros. Consentimiento inequívoco, libre e informado que permite a la persona a la que se refieren autodeterminarse informativamente. No obstante, es claro que en ciertas ocasiones ha de ser posible tratar información personal sin que medie la autorización del afectado. Por eso, y aquí viene el segundo elemento, la ley puede autorizarlo expresamente, bien de forma general, al darse las circunstancias por ella previstas, o caso por caso. Así, consentimiento y habilitación legal son los títulos que justifican el tratamiento de datos personales.

Ahora bien, que, por mediar cualquiera de ellos, sea lícito recogerlos y utilizarlos no significa que el afectado pierda su capacidad de autodeterminación en este ámbito. Al contrario, dispone de una serie de facultades –de derechos– que completan su poder de disposición y de control, empezando por el de revocar la autorización cuando la hubiere prestado. Facultades que tienen por objeto ejercer su poder de consentir el tratamiento de sus datos con pleno conocimiento de las consecuencias de su decisión y, luego, reaccionar contra quienes hagan un uso indebido de ellos.

Así, integran el contenido activo de este derecho las siguientes facultades: 1) ser informado en la recogida de datos; 2) conocer la existencia de ficheros y tratamientos de datos personales; 3) acceder a ellos para comprobar qué información personal del afectado contienen; 4) obtener la rectificación de los que no sean exactos; 5) obtener la cancelación de los que no deban ser tratados o hayan perdido la calidad que en su día justificó el tratamiento; 6) oponerse a un tratamiento cuando no sea necesario conforme a la ley el consentimiento del afectado y concurran motivos fundados y legítimos relativos a su concreta situación personal; 7) no sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente; 8) ser resarcido de los sufridos a causa de tratamientos que no se ajusten a las condiciones legalmente establecidas; 9) ser protegido por las instituciones especializadas creadas *ex profeso* para defender este derecho fundamental.

A su vez, estas facultades constituyen el reverso de los deberes y obligaciones que pesan sobre quienes efectúan tratamientos de datos personales y, en último caso, sobre las agencias de protección de datos.

En fin, la tipificación como delito o infracción administrativa de las conductas que vulneran más gravemente el

derecho a la autodeterminación informativa completa su régimen jurídico esencial.

2. Las circunstancias que nos han traído hasta aquí

A este resultado se ha llegado como consecuencia de la convergencia de una pluralidad de factores.

Pueden variar en cada una de las experiencias nacionales los elementos que entran en juego así como las modalidades y términos del reconocimiento del derecho, pero son comunes, al menos, los siguientes: a) la creciente informatización de la sociedad en los países avanzados y el avance vertiginoso de las tecnologías de la información y de las comunicaciones (TIC); b) la circulación cada vez más intensa de personas, bienes y servicios, especialmente, pero no de modo exclusivo, en el seno de la Unión Europea; c) la virtualidad de esas tecnologías para canalizar relaciones de todo tipo dentro y fuera de los Estados; d) las posibilidades que ofrecen para la injerencia en la vida ajena por parte del poder público o de sujetos privados; e) la utilidad que representan como instrumento de control y de seguridad en manos de los gobernantes; f) el valor económico directo o indirecto que han adquirido los datos personales; g) la reivindicación desde diversos sectores, no mayoritarios y, preferentemente, intelectuales y comprometidos con los derechos humanos, de instrumentos de tutela jurídica contra los potenciales peligros que traen consigo esas tecnologías para las personas.

En España, la respuesta fue tardía en comparación con otros países que comenzaron a reaccionar frente a esos riesgos ya a principios de los años setenta. Y si después hemos avanzado con más rapidez, no se debe olvidar que la previsión efectuada por el artículo 18.4 de la Constitución permitía esperar una actuación del legislador más diligente y, sobre todo, debida a razones digamos de libertad. Sin embargo, lo que determinó el cumplimiento del mandato constitucional fue la incorporación de España al espacio previsto en los Acuerdos de Schengen y la correlativa exigencia de dotarse de una normativa de protección de datos personales. Pero, desde la Ley Orgánica 5/1992, hasta la Sentencia del Tribunal Constitucional 292/2000 que reconoce el derecho fundamental, se han sumado los siguientes elementos, cuya concurrencia explica el sentido de ese pronunciamiento:

1.º) El debate de intensidad creciente promovido desde ámbitos académicos y sociales sobre el bien jurídico que protegía esa legislación y, en particular, sobre la diferencia existente entre intimidad y autodeterminación informativa.

2.º) La progresiva elaboración en el espacio europeo, a partir del Convenio del Consejo de Europa n.º 108, de una disciplina orientada a proteger los datos personales, que acabará plasmada en la Directiva 95/46.

3.º) El paso dado por la Unión Europea en el 2000 con la Carta de los Derechos Fundamentales al reconocer la autonomía del derecho a la protección de datos de carácter personal.

4.º) La jurisprudencia del Tribunal Europeo de Derechos Humanos que, a partir del derecho a la vida privada reconocido por el artículo 8 de la Convención, dotó de autonomía a la protección de datos de carácter personal (casos Amann contra Suiza y Rotaru contra Rumania, ambos del 2000).

5.º) La dinámica generada por la aplicación de una Ley –la LORTAD– que expresamente hablaba de un nuevo derecho fundamental, y por la jurisprudencia constitucional que, en sintonía con posiciones doctrinales, iba acentuando la autonomía de la técnica jurídica de la protección de datos personales respecto del derecho a la intimidad.

Bajo todas estas premisas, la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, interpretando el artículo 18.4 de la Constitución, a la luz del Convenio n.º 108 del Consejo de Europa, conforme lo quiere el artículo 10.2, también del texto de 1978, dio el paso de reconocer el derecho fundamental a la protección de datos de carácter personal, opción cuya importancia es manifiesta y que, más allá de su decisivo significado jurídico, destacado por todos los intérpretes, ha merecido algunas críticas, sea por el lugar en que ha asentado ese derecho fundamental (el citado artículo 18.4), sea por los términos en los que lo ha reconocido (Martínez Martínez, 2004).

En definitiva, los riesgos del avance tecnológico, el diálogo entre la doctrina, el legislador y los jueces, así como el trasfondo europeo, junto a la virtualidad de la interpretación constitucional (Lucas Murillo de la Cueva, 2003) explican que hayamos llegado hasta aquí y, también, que

vayamos conociendo cada vez mejor las distintas facetas y aspectos del derecho a la autodeterminación informativa, entre ellos sus conexiones y diferencias con otros derechos fundamentales, particularmente, con los que se sitúan en el plano más próximo a la personalidad.

3. Las perspectivas

Los progresos que se van dando en materia de derechos son ciertamente conquistas importantes, pero, una vez alcanzados, se convierten en el punto de partida para lograr nuevos retos, nuevas aspiraciones. Por otro lado, el reconocimiento de un derecho por sí mismo no basta para asegurar su efectiva realización. Estas observaciones, válidas con carácter general, sirven también en relación con el derecho a la protección de datos de carácter personal. Son, incluso, especialmente significativas porque ha sido alumbrado recientemente y porque guarda relación estrecha con un proceso de transformación de las relaciones sociales a impulsos del progreso tecnológico que está en plena materialización.

Resulta, a propósito de lo primero, que las leyes, al menos las dictadas en España, han trazado un marco general de protección de datos que, si bien tiene la ventaja de contar con normas abiertas susceptibles de ser aplicadas a una multiplicidad de supuestos de hecho, en cambio, tiene que afrontar la dificultad que representan las particularidades de algunos ámbitos especialmente complejos, necesitados, por tanto, de una consideración singular, con la que no contamos. Por citar algún ejemplo, cabe mencionar, en ese sentido, el régimen de los ficheros y tratamientos de datos de carácter personal de los juzgados y tribunales, sobre el que hay una sucinta previsión legal (los artículos 230 y 235 de la Ley Orgánica del Poder Judicial) y una insuficiente regulación reglamentaria (recogida en el Reglamento sobre aspectos accesorios de las actuaciones judiciales) que propicia algunas controversias que, de otro modo, no se plantearían (SSTS de 18 y 19 de septiembre y de 30 de octubre de 2006 –recursos 74/2003, 274/2002 y 183/2003, respectivamente–).

Asimismo, se ha insistido en la falta de coordinación existente entre las normas que regulan la protección de datos de carácter personal y las dedicadas por la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, al acceso a los registros y archivos públicos previsto por el artículo 105 b) de la Constitución. Aspecto éste que adquirirá nuevos perfiles cuando entre en vigor la Ley para el Acceso Electrónico de los Ciudadanos a las Administraciones Públicas, actualmente pendiente de aprobación por el Congreso de los Diputados. Y también se ha llamado la atención sobre la necesidad de contar con previsiones que tengan en cuenta las características de los datos relativos a la educación y a la enseñanza, ámbitos en los que se han producido algunos conflictos a propósito de la publicación de calificaciones de los alumnos y de las evaluaciones de la labor docente e investigadora de los profesores universitarios (Troncoso Reigada, 2006).

Problemas que ha querido resolver la Ley Orgánica 4/2007, de modificación de la de Universidades, que autoriza la publicación de las calificaciones de los alumnos y de los resultados de la evaluación de la labor docente e investigadora de los profesores, al tiempo que requiere al Gobierno para que regule los *currículum* de profesores e investigadores. Por su parte, la Ley Orgánica 2/2006, de Educación, ha establecido algunas previsiones específicas en su disposición adicional vigésimo tercera, sobre el tratamiento de los datos de los alumnos. Una y otra se remiten, por lo demás, al régimen general establecido por la LOPD.

Hasta hace relativamente poco tiempo, otro de los sectores para los que se reclamaban reglas específicas era el de los *datos relativos a la salud*. No obstante, la Ley 41/2002, básica reguladora de la autonomía del paciente, afrontó ese problema, aunque su regulación suscite algunos interrogantes de importancia.

Consideraciones no muy distintas habría que hacer respecto de algunos ficheros y tratamientos realizados por sujetos privados. Sería el caso de los que se llevan a cabo en el ramo de los seguros, la *solvencia y crédito* o en el marco de las *relaciones laborales*.

Ahora bien, la solución a la que está recurriendo el legislador cuando contempla la cuestión de la protección de datos en campos específicos (órganos jurisdiccionales, telecomunicaciones, servicios de la sociedad de la información, firma digital, educación, universidades) ha consistido, fundamentalmente, en remitirse a la ley general sin aportar más que algunas previsiones muy concretas, aunque puedan ser muy relevantes, como especificar algunos derechos y atribuir potestad sancionadora a la Agencia Española de Protección de Datos en materia de servicios

de la sociedad de la información y comercio electrónico (Ley 34/2002) y de telecomunicaciones (Ley 32/2003).

A lo que se ha dicho, debe añadirse que lo reciente y lo novedoso de la materia implica desconocimiento de su importancia no sólo por los ciudadanos, sino también por quienes están al frente de las instituciones. Esto último es particularmente grave porque, a casi quince años de la publicación de la Ley Orgánica 2/1992, no puede considerarse satisfactorio el cumplimiento por parte de las administraciones de las exigencias propias de la legislación sobre protección de datos o que no se haya procedido a dictar los reglamentos de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal y permanezcan en vigor los aprobados conforme a la LORTAD, a pesar de que han transcurrido ya más de siete años de la derogación de ésta por aquélla.

Y, si esto sucede con los poderes públicos que están doblemente vinculados por la Ley, positiva y negativamente, se debe comprender que los ciudadanos desconozcan todavía los riesgos a que se exponen como consecuencia del uso por terceros de sus datos personales y, por tanto, no tengan conciencia de que deben luchar por los derechos que para su protección tienen reconocidos. Esa limitada lucha de los ciudadanos por los derechos de autodeterminación informativa hace que la labor de los Tribunales –y anteriormente de la Agencia Española de Protección de Datos– se vea condicionada por el relativamente escaso número de recursos –reclamaciones en el caso de la Agencia– que les llegan, aunque eso no les haya impedido dictar sentencias y resoluciones de gran importancia para abrir espacios, reforzar los límites de la actuación de las administraciones en relación con los datos personales y poner freno a abusos y excesos cometidos por particulares, empresas en especial, que se dedican a su tratamiento o se valen de los realizados por otros.

Las perspectivas que tenemos abiertas son, por tanto, contradictorias. De un lado, reflejan el aspecto positivo representado por la existencia de un reconocimiento del carácter fundamental del derecho, junto con un marco jurídico general europeo y estatal que lo desarrolla, así como por la actuación cada vez más eficaz de autoridades independientes de control y la tutela decidida prestada por los tribunales de justicia. Pero, de otro, expresan las insuficiencias relacionadas con la carencia de regulaciones sectoriales y la falta de una efectiva observancia de los principios y derechos de la autodeterminación informativa en muchos espacios. Y, en consecuencia, el enorme trabajo que queda por hacer para superar tal estado de cosas.

Estas consideraciones generales deben ser acompañadas por otras referidas separadamente al ámbito público y al privado, las cuales deben tener presente que las relaciones que tienen lugar dentro de cado uno y entre ellos se producen y se producirán, cada vez más, a través de medios electrónicos. A ese respecto, el fenómeno de Internet y de las otras formas o canales de comunicación que hacen posible las TIC suscitan problemas y dificultades de particular importancia en ambos planos.

4. El dominio público. La eficacia, la eficiencia y la seguridad

Mencionaba antes el Proyecto de Ley de Acceso Electrónico a las Administraciones Públicas, en avanzado estado de tramitación legislativa. Este proyecto contiene el reconocimiento del derecho de los ciudadanos a relacionarse con la Administración y recibir comunicaciones de ella por medios electrónicos. Al mismo tiempo, contempla la regulación del procedimiento administrativo por medios electrónicos y quiere que, para el 31 de diciembre del 2009, todas las administraciones –la Administración General del Estado, las autonómicas y las locales– estén en condiciones de hacer posible, en todos los procedimientos, el derecho a acceder electrónicamente a ellas.

Las posibilidades que la administración electrónica ofrece en términos de eficacia y eficiencia son evidentes. Como apunta la exposición de motivos del proyecto, no sólo servirán para superar o relativizar las barreras que suponen el tiempo y el espacio a la hora de obtener servicios públicos o de formular todo tipo de reclamaciones, sino que, a la vez, harán posible que los ciudadanos obtengan respuestas con una rapidez desconocida. De este modo, las administraciones ganarán un grado de cercanía efectiva del que ahora carecen. En este sentido, las aspiraciones del proyecto son muy ambiciosas y cuando se conviertan en realidad significarán un cambio cualitativo en la actuación de los poderes públicos en sus relaciones internas y externas. Cambio del que, en la actualidad, contamos con muestras elocuentes en aspectos que van más allá de la muy generalizada oferta de información, como es, por

ejemplo, la que ofrece la Agencia Estatal de la Administración Tributaria en relación con la declaración y liquidación de tributos (en virtud de lo previsto por la Ley General Tributaria).

No obstante, a las ventajas que ese objetivo comporta van unidas dificultades de entidad. El proyecto se remite a la LOPD en cuanto a la protección de los datos personales y, en coherencia con lo que en ella se dispone, exige el consentimiento del afectado o autorización legal para recabar de las distintas dependencias donde se hallen los documentos precisos, que el interesado, conforme al artículo 35 de la Ley 30/1992, no tiene por qué aportar. También limita su utilización al procedimiento de que se trate y exige que se observen las medidas de seguridad necesarias a la hora de la conservación y custodia del expediente electrónico. No contiene, sin embargo, criterios específicos sobre cesiones o comunicaciones de datos personales en las relaciones administrativas ni tampoco respecto del acceso por terceros a esos expedientes y a los registros electrónicos correspondientes. Sobre lo uno y lo otro habrá que estar a las normas de la LOPD y de la Ley 30/1992.

Se ha dicho que la exigencia de autorización legal para que, en ausencia de consentimiento del afectado, las administraciones puedan efectuar comunicaciones de los datos personales es un exceso en el que habría incurrido el Tribunal Constitucional al declarar la nulidad de la parte del artículo 21 de la LOPD, que consideraba suficiente para ello que lo previera la disposición de creación del fichero o, en general, una norma reglamentaria. No estoy seguro de que quepa tachar de exceso ese pronunciamiento. En cambio, sí que me parece conveniente imponer límites estrictos a las administraciones respecto del uso de los datos de que disponen aunque sea para el ejercicio de las funciones que tienen conferidas. Asimismo, creo que las normas de la LOPD sobre el consentimiento y sobre aquellos otros supuestos en los que exime de su prestación expresa por considerarlo implícito, ofrecen un margen importante, al igual que lo suministran las distintas normas legales atributivas de potestades a esas administraciones. Desde uno y otro frente, debe obtenerse espacio suficiente para llevar a cabo las comunicaciones que sean imprescindibles.

En cuanto al acceso, no por el afectado, sino por terceros interesados a los expedientes, archivos y registros administrativos, la Ley 30/1992 lo circunscribe de manera que el respeto al derecho a la intimidad se convierte en uno de los límites al mismo. Y también excluye la solicitud de acceso genérica o generalizada, al tiempo que restringe ese acceso por terceros a documentos nominativos que, sin referirse a aspectos íntimos, contengan datos de carácter sancionador o disciplinario a quienes lo pretendan para el ejercicio de un derecho, siempre que acrediten un interés legítimo y directo. Los cuales deberán solicitarlo individualmente, pudiendo ser denegado, motivadamente, además de cuando lo prevea la Ley, en los casos en que deban prevalecer razones de interés público o derechos de terceros más dignos de protección. Normas todas éstas que vienen siendo precisadas por la jurisprudencia que ha admitido, por ejemplo, como no lesivo del derecho a la autodeterminación informativa el traslado del expediente a los interesados que son parte en un procedimiento administrativo [STS de 26 de octubre de 2005 (casación 5173/2001)] o el acceso a los ejercicios de otros aspirantes en procedimientos competitivos para el ingreso en las administraciones públicas [STS de 6 de junio de 2005 (recurso 68/2002)]. Y ha rechazado pretensiones de acceso masivas o genéricas [STS de 19 de mayo de 2003 (casación 3193/1999)].

De esta manera, siguiendo criterios razonables y atendiendo a las previsiones legales, el espacio que queda es menos amplio de lo que pudiera parecer. Por otro lado, cabe considerar que el artículo 37 de dicha ley ofrece el soporte legal necesario para consentir un acceso puntual por terceros a datos personales de otros y que, incluso, suministra a las administraciones públicas fundamento para delimitarlo. Esta impresión no es compartida, sin embargo, por quienes opinan, con argumentos respetables –entre ellos el que apunta al distinto peso de un derecho fundamental y de un interés legítimo–, que es imprescindible abordar una regulación que armonice satisfactoriamente el derecho a la autodeterminación informativa con el de acceder a los archivos y registros públicos (por ejemplo, Fernández Salmerón, 2003).

Con todo, no me parece que los problemas más graves vengan desde esta dirección. Me parecen más preocupantes los que tienen que ver con el cumplimiento real de las medidas de seguridad, con poner término a los accesos y comunicaciones ilegales de datos o con evitar procedimientos de eliminación de documentación consistente en arrojar a la basura expedientes completos o historias clínicas. En este plano, la formación de los funcionarios es imprescindible, de igual modo que la exigencia de responsabilidad disciplinaria siempre que proceda.

Asimismo, me parece importante prevenir e impedir excesos con el pretexto de la protección de la seguridad pública. El afán por acopiar por todos los medios disponibles información relevante para combatir, sobre todo, el terrorismo se ha hecho sentir con gran fuerza después del 11 de septiembre de 2001 y ha llevado a que, especialmente en Estados Unidos, se hayan creado bases de datos de carácter personal que incluyen, incluso, los de carácter sensible, y son gestionadas al margen de todo sistema de control efectivo por parte de los afectados o de instancias independientes. Un ejemplo del que han venido informando los medios de comunicación es el relativo a la recopilación en secreto de datos financieros y de transacciones bancarias de ciudadanos de diversas nacionalidades a partir de una empresa belga que canaliza diariamente millones de operaciones bancarias mediante un programa denominado Swift, operado por el Departamento del Tesoro (*New York Times* de 23 de junio del 2006). Y también se puede mencionar el programa de vigilancia sobre las telecomunicaciones Echelon.

El riesgo de la utilización de los ingentes recursos que las nuevas tecnologías ofrecen a este respecto se ha proyectado, incluso, en controversias que han llegado a plantearse jurisdiccionalmente, como es el caso de los datos personales sobre pasajeros de líneas aéreas que viajan a América del Norte que han de ser suministrados a la Administración estadounidense. Conflicto al que se le dio una solución que no todos vieron como satisfactoria desde el punto de vista del ordenamiento comunitario en materia de movimientos internacionales de datos personales, luego anulada por la Sentencia de 30 de mayo de 2006 del Tribunal de Justicia de las Comunidades Europeas si bien por motivos de carácter competencial y, por tanto, ajenos al derecho a la autodeterminación informativa. En la actualidad la cuestión está pendiente de la negociación de un nuevo acuerdo entre Estados Unidos y la Unión Europea.

Otro plano en el que se han suscitado interrogantes es el que tiene que ver con la introducción de *nuevas obligaciones para las empresas que prestan servicios de telecomunicaciones* sobre las llamadas que realicen sus abonados. Iniciativas que van en la línea de las medidas ya previstas en ese sentido por el artículo 12 de la Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico, para operadores de redes y servicios, proveedores de redes de acceso a telecomunicaciones y prestadores de servicios de alojamiento de datos, que les obligan a retener y conservar durante doce meses los de conexión y tráfico de comunicaciones realizadas durante la prestación de un servicio de los contemplados por ese texto legal. Previsión legal que se preocupa, no obstante, de precisar que, en ningún caso, se extiende esa obligación al contenido de las comunicaciones.

La Directiva 2002/58, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), se limitó a autorizar a los Estados a obligar, por ley y para proteger la seguridad nacional y la seguridad pública, entre otras razones, a conservar por un plazo determinado los datos personales relativos a las comunicaciones electrónicas (artículo 15.1). Pero la Directiva 2006/24, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, la ha modificado en parte y ha desarrollado este aspecto.

Responde a la necesidad de armonizar las legislaciones estatales en la materia ante el crecimiento de las comunicaciones electrónicas y la necesidad de combatir la delincuencia organizada y, particularmente, el terrorismo. No en vano, tras los atentados de Londres de julio del 2005 se anunciaron por diversos gobernantes medidas del tipo de las ahora adoptadas y en los considerandos de este texto se hace referencia expresa a ellos. Es de destacar que la regulación recogida en esta nueva directiva parte del mismo principio ya adoptado para las comunicaciones relativas al comercio electrónico: la obligación de conservar los datos no se refiere al contenido de la comunicación sino solamente a aspectos externos a ella. Es decir, a los generados o tratados en el proceso del suministro de servicios de comunicación. Más en concreto, se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los relacionados necesarios para identificar al abonado o al usuario registrado. Y quedan incluidos los correspondientes a las llamadas infructuosas. El período de conservación se fija entre seis meses y dos años, ampliables si median circunstancias especiales, durante el cual podrán acceder a esta información las autoridades competentes, conforme a la legislación de cada Estado.

Es el legislador estatal quien ha de regular los términos concretos en los que la información relativa a las comunicaciones ha de ser conservada y de qué manera podrán acceder a ella las autoridades competentes. La directiva,

consciente de lo delicado de esta materia, le hace advertencias explícitas y reiteradas sobre los extremos que debe tener presente al realizar esa tarea. En efecto, advierte que ese acceso solamente podrán realizarlo dichas autoridades respetando los derechos fundamentales de las personas afectadas y observando el principio de proporcionalidad. Igualmente, demanda medidas de seguridad para evitar que accedan quienes no deban a estos datos, y requiere sanciones para quienes lo hagan indebidamente. De igual modo, asegura el derecho al resarcimiento, conforme a la Directiva 95/46 a quienes sufran como consecuencia de tratamientos ilícitos o de acciones incompatibles con las legislaciones internas que han transpuesto esa directiva.

La preocupación que expresa la directiva por circunscribir los márgenes en los que ha de moverse el legislador interno ya nos advierte de que detecta serios riesgos en las medidas de conservación y puesta a disposición de las autoridades competentes de estos datos. Y eso a pesar de que quedan excluidos expresamente los relacionados con el contenido de las comunicaciones. Pero los vinculados al origen y destino (intervinientes), fecha, hora y duración, tipo de comunicación, equipo de los usuarios y su localización son suficientemente significativos desde la perspectiva no sólo del derecho a la autodeterminación informativa sino de otros derechos fundamentales como para despertar las alarmas.

Naturalmente, esto significa que habrá que examinar con el mayor cuidado la forma en que las Cortes Generales van a transponer al ordenamiento español esta directiva. El proyecto de ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, actualmente en trámite en el Congreso de los Diputados se dirige a tal fin (Boletín Oficial de las Cortes Generales. Congreso de los Diputados, Serie A, n.º 128-I, de 16 de marzo de 2007). Lo delicado de la materia lo reconoce el propio texto, que se preocupa por resaltar reiteradamente que queda a salvo de las medidas que contempla el contenido de las comunicaciones y que las cesiones de los datos que obliga a conservar solamente se producirán con autorización judicial. Ahora bien, eso no le impide extender la obligación de cederlos, aunque sea con esa garantía, a los relevantes para la investigación de cualquier delito y no sólo de los graves, que es lo que considera la directiva. La exposición de motivos del proyecto explica que esa extensión está permitida por la directiva, guarda relación con el régimen del secreto de las comunicaciones y es aconsejable, ya que, muy a menudo, cuando comienza una investigación criminal no se percibe el alcance que llegará a tener y que, de este modo, no se cercenan las posibilidades puestas a disposición de la autoridad judicial para detectar las responsabilidades penales.

El articulado precisa que los obligados a conservar los datos son los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones (artículo 2), indica los datos que deben ser conservados en los términos previstos por la directiva (artículo 3), incluyendo los relativos a las llamadas infructuosas (artículo 4) y durante cuánto tiempo: doce meses, plazo que reglamentariamente puede ampliarse hasta dos años o reducirse hasta seis meses para determinados datos (artículo 5). En cuanto a la cesión (artículos 6 y 7), precisa que solamente cabe efectuarla, previa autorización judicial que determinará el alcance de la misma, a los agentes facultados y que éstos son (artículo 6.2)) los miembros de las Fuerzas y Cuerpos de Seguridad del Estado cuando actúen como policía judicial y los del Centro Nacional de Inteligencia en el curso de investigaciones sobre personas o entidades en el marco de lo previsto en la Ley 11/2002, de 6 de mayo, que lo regula y en la Ley Orgánica 2/2002, de la misma fecha, que regula el control judicial previo de sus actividades. También tendrán la consideración de agentes facultados los funcionarios de la Dirección Adjunta de Vigilancia Aduanera cuando actúen como policía judicial.

El plazo para efectuar la cesión, dice el proyecto, será fijado por los agentes facultados atendiendo a la urgencia y a la naturaleza y complejidad técnica de la operación. En todo caso, señala para los supuestos en los que no se fije el de cuarenta y ocho horas para datos de antigüedad inferior a tres meses y el de setenta y dos horas para los que la superen (artículo 7.3). La cesión se realizará en formato electrónico de acuerdo con las particularidades que deberán establecer conjuntamente en el plazo de tres meses desde la entrada en vigor de la ley los Ministerios de Interior, Defensa y Economía y Hacienda. Y correrá a cargo de los sujetos obligados la configuración de sus equipos y la actualización técnica necesarias para cumplir las obligaciones de conservación y cesión de datos (disposición final cuarta).

Completan las normas especiales incluidas en el proyecto las relativas a la protección y seguridad de los datos, las excepciones a los derechos de acceso y cancelación y las correspondientes a las infracciones y sanciones. En cuanto a lo primero, el artículo 8 efectúa varias remisiones a la LOPD y reitera que la Agencia Española

de Protección de Datos es la responsable de velar por su cumplimiento. Más importantes son las previsiones del artículo 9, que excluyen el deber de los responsables de los tratamientos de comunicar las cesiones y les obligan a denegar el ejercicio del derecho de cancelación a quien sea objeto de investigación de un delito o sus datos hayan sido cedidos conforme a lo previsto en esta normativa. Al mismo tiempo, reconocen a los afectados que vean denegadas en todo o en parte sus pretensiones de cancelación, el derecho a ponerlo en conocimiento de la Agencia Española de Protección de Datos, la cual deberá asegurarse de la procedencia o improcedencia de la denegación. Finalmente, en materia sancionadora, el proyecto se remite a la Ley 32/2003, varios de cuyos preceptos modifica la disposición adicional única.

Hay, además, otras novedades, como la aportada por la disposición adicional única del proyecto en materia de identificación de las personas que adquieran tarjetas de prepago para los servicios de telefonía móvil. Identificación que deberán efectuar los operadores que comercialicen esos sistemas de activación para lo cual se les exige llevar un libro-registro y conservar los datos correspondientes durante la vigencia de la tarjeta y hasta que transcurran los plazos previstos en el proyecto, así como cederlos a los agentes facultados. Obligaciones éstas cuyo incumplimiento se castiga también conforme a lo previsto en la Ley 32/2003, según la modificación que en ella se introduce.

Es pronto para avanzar un juicio preciso sobre este régimen añadido. Parece que, en lo sustancial, el proyecto se ajusta a la Directiva y que comparte con ella, como no podía ser de otro modo, la preocupación por mantener un equilibrio entre las intervenciones que introduce y las garantías del secreto de las comunicaciones y del derecho a la autodeterminación informativa. La opción por extender las nuevas obligaciones a todos los casos de investigaciones por delito, con independencia de que la autorice la directiva, no es, en mi opinión, especialmente significativa. Lo más importante será controlar la utilización de estos instrumentos para limitarla a aquellos supuestos en los que esté justificado su uso y asegurar que se observan los plazos de conservación y las medidas de seguridad de los datos para que, efectivamente, no acceda a ellos quien no deba y en ningún caso se aprovechen para fines distintos de los previstos legalmente. Para ello, la Agencia Española de Protección de Datos y los jueces deberán ser especialmente exigentes porque estas medidas pueden afectar, no ya al derecho a la autodeterminación informativa y al derecho al secreto de las comunicaciones, sino a la propia libertad de las personas.

Por eso, no está de más recordar que, en efecto, los poderes públicos deben velar por la seguridad de todos, especialmente frente a la amenaza terrorista y las formas de criminalidad organizada. Y que deben servirse para ello de todos los medios disponibles entre los que destacan por su eficacia los que suministran las tecnologías de la información y las comunicaciones y permiten acopiar datos personales. Pero, al mismo tiempo y con el mismo énfasis, ha de tenerse presente que una cosa es que se sirvan de ellos para prevenir los delitos y perseguir a los delincuentes y otra distinta que procedan a registrar y tratar al margen de todo control la vida y obras de millones de personas sin relación alguna con tales conductas. La legislación vigente no lo permite. De lo que se trata es de que siga siendo así y de que cambios normativos, como el que está en ciernes y los que se puedan introducir en el futuro, si las circunstancias los exigieren, se hagan dentro del más estricto respeto a los principios que rigen, no ya en esta materia, sino, en general, en relación con los derechos y libertades de los ciudadanos. Para ello, no basta con el cuidado del legislador ni con el celo del gobernante. Es decisiva la vigilancia de los órganos e instituciones de garantía sobre quienes están encargados de aplicar las leyes.

Decía que, hasta ahora, no se han suscitado especiales problemas a propósito de los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado. Incluso, pueden apuntarse episodios que han puesto de manifiesto un buen funcionamiento del sistema de garantías creado por el legislador en este ámbito, como sucedió con la Circular 1/1997 de la Dirección General de Policía que dictaba instrucciones sobre «Captación de datos de interés para la Seguridad Ciudadana» (Del Castillo Vázquez, 2007). Según ellas, la Policía debía hacerse con datos sin que mediaran elementos que hicieran pensar en la posibilidad de una actuación delictiva, bastando con la simple curiosidad o sospecha de los agentes. Asimismo, se mencionaban las fuentes de información potenciales (entidades vecinales, vecinos, comerciantes, familiares, empresas de seguridad privada) y se estimaban informaciones de interés aquellas relativas a inquilinos, locales frecuentados por menores en los que se consumían bebidas alcohólicas, vehículos que circulaban a determinadas horas por el barrio y que pudieran dedicarse al tráfico de drogas, anuncios de alquiler de viviendas y comportamientos de personas no habituales que hubieren llamado la atención de algún vecino.

Esa circular suscitó críticas desde una asociación judicial y originó una pregunta en el Senado, ante lo cual el Ministerio del Interior optó por retirarla aduciendo en justificación de esa decisión su «redacción confusa» y que «su aplicación podría hacer llegar a la conclusión de que se estaban vulnerando determinados conceptos unidos al derecho fundamental a la protección de la intimidad».

En definitiva, no debe perderse de vista la idea central de que la mejor manera de defender los principios del estado de derecho, del que forman parte inescindible los derechos fundamentales, es respetándolos también a la hora de hacer frente al terrorismo y a la delincuencia organizada, lo cual exige observar escrupulosamente los procedimientos constitucionales que permiten limitarlos y los márgenes en los que es posible hacerlo. La supresión de las garantías sin esas cautelas o, en general, la creación de espacios inmunes al control parlamentario y judicial, a la larga solamente conduce a resultados contrarios a los perseguidos.

5. El dominio privado

Al estudiar la LORTAD me llamó la atención la amplitud de las excepciones que establecía en relación con el tratamiento de datos personales desde ficheros de titularidad pública (Lucas Murillo de la Cueva, 1993). Años más tarde (Lucas Murillo de la Cueva, 2000), tuve la impresión de que la LOPD, no sólo no corrigió esa disposición permisiva respecto de los poderes públicos, sino que la acompañó con la apertura de huecos a través de los que operadores privados podrían hacerse con datos de carácter personal y tratarlos sin consentimiento del afectado o más allá de los términos en los que éste fue concedido. Pensaba, sobre todo, en el cambio introducido en el artículo 4.2 de la LOPD, que permite utilizarlos para *finalidades distintas* de las que motivaron su recogida siempre que no sean incompatibles con él –la LORTAD prohibía su uso para fines distintos– y en la figura del *censo promocional*, fuente accesible al público, anunciada por la Ley 7/1996, de Ordenación del Comercio Minorista, que hace posible sortear la prohibición de acceso y utilización de los datos del censo electoral (artículo 31 LOPD).

Afortunadamente, el Tribunal Constitucional ha eliminado los excesos más llamativos con los que el legislador ha querido facilitar el tratamiento de datos personales por parte de las administraciones públicas (STC 292/2000) declarando la nulidad, por inconstitucionales, de parte de los artículos 21.1 (comunicación de datos entre administraciones públicas) y 24 (información en la recogida de datos y ejercicio de los derechos de acceso y rectificación ante los ficheros de titularidad pública). Por lo que se refiere a las mencionadas normas pensadas para facilitar los tratamientos desde el sector privado, aunque permanecen vigentes, la Audiencia Nacional y el Tribunal Supremo –que viene confirmando su interpretación de la LOPD– han reducido a la inoperatividad ambos cambios aportados por el legislador de 1999.

El primero, porque ha venido a equiparar las finalidades incompatibles con las diferentes a la que justificó la captación de los datos [SAN de 8 de febrero de 2002 (recurso 1067/2000, seguida posteriormente por otras)]. El segundo, porque ha negado virtualidad al artículo 39.3 de la Ley 7/1996, de Ordenación del Comercio Minorista, para hacer accesibles los datos del censo electoral, cuya prohibición de tratamiento mantiene en tanto la Ley Orgánica del Régimen Electoral General no disponga otra cosa [recientemente, STS de 7 de marzo de 2006 (casación 1728/2002), que recoge otras anteriores a partir de la STS de 18 de octubre de 2000]. Asimismo, en otros puntos estrechamente relacionados con el tratamiento de datos por sujetos privados, la jurisprudencia está siendo especialmente rigurosa. Es lo que sucede en cuanto a la exigencia del *consentimiento*, que no permite entenderlo concedido por la falta de manifestación del afectado en sentido contrario tras la comunicación de un sujeto privado de que se propone tratar sus datos de no recibir comunicación en contra [STS de 18 de marzo de 2005 (casación 7707/2000)]; y de la *finalidad determinada*, que excluye la validez de las formuladas en términos genéricos [STS de 11 de abril de 2005 (casación 4209/2001)]. O cuando limita a sus estrictos términos legales el concepto de *fuente accesible al público* [STS de 20 de febrero de 2007 (casación 732/2003)] y exige que los responsables de los ficheros y tratamientos velen por la *calidad de los datos*, depurando los inexactos y no puestos al día [STS de 18 de julio de 2006 (casación 322/2005)].

No obstante, esa proclividad del legislador hacia el sector privado me parece preocupante. Y es que, al fin y al cabo, el ámbito o dominio público está sujeto a límites y restricciones que no vinculan a los particulares. Eso explica que, a veces, sin necesidad de recurrir a los remedios especiales previstos por la LOPD, sino mediante los instrumentos ordinarios de control de la actuación del poder ejecutivo, es decir, haciendo efectivas las exigencias a las que la ley

somete la producción de actos administrativos o la elaboración de disposiciones generales, sea posible eliminar aquellos que se consideren contrarios al derecho que examinamos. Así, la STS de 28 de marzo de 2007 (recurso 76/2005), declaró la nulidad de los artículos 323.1 y 2 y 324 del Reglamento del Registro Mercantil (Real Decreto 685/2005) sobre publicidad vía Internet de resoluciones judiciales sobre deudores concursados por falta de dictamen del Consejo de Estado sobre la redacción finalmente aprobada. Y, desde el punto de vista de los controles parlamentarios, el caso antes relatado de la Circular 1/1997 de la Dirección General de la Policía muestra otro medio, no especializado, de limitar la acción pública en defensa también del derecho a la autodeterminación informativa.

En el ámbito privado, en cambio, esas restricciones y condicionamientos jurídicos e institucionales no existen. Y, sin embargo, los datos de carácter personal constituyen un bien cada vez más valioso económicamente por las posibilidades que su conocimiento y su elaboración ofrecen para las más variadas actividades. Eso hace que se demanden con creciente intensidad y que se redoblen los esfuerzos por captarlos y someterlos a tratamientos que lleven a un conocimiento más específico de las personas a las que pertenecen. Captación que no siempre se hace informando al afectado sobre los términos en los que se le pide el consentimiento, si es que se le solicita. Y tratamientos que pueden no respetar la finalidad que originó la recogida de unos datos determinados. Además, es un mundo mucho más opaco. Quiero decir que los actores que se mueven en él no hacen ostentación de la disposición de esa información personal, simplemente, la utilizan.

Si a esto unimos todo cuanto antes se decía sobre la todavía escasa conciencia de los peligros relacionados con la utilización por terceros de información personal y con el deficiente conocimiento de los instrumentos jurídicos pensados para proteger a los afectados, nos podremos hacer una idea más cabal de la entidad de los problemas que tenemos ante nosotros. Especialmente, en un contexto donde, sea a través de la televisión interactiva, la telefonía o Internet, los particulares exponen datos que les conciernen ante muy variados operadores, que pueden hacerse con ellos con gran facilidad sin que el usuario lo perciba.

No hay duda de que la Agencia Española de Protección de Datos es consciente de todo esto y que se esfuerza en advertir de los riesgos que implican el acceso y tratamiento incontrolados de datos personales por terceros y en informar sobre los medios para impedirlos. En este sentido, no hay duda de que lleva y ha llevado a cabo actuaciones muy importantes en relación con los ficheros de solvencia y crédito. Se han plasmado, además de en su labor inspectora y sancionadora, en la Instrucción 1/1995, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito [cuya legalidad ha confirmado la STS de 16 de febrero de 2007 (casación 220/2003)].

No obstante, la tarea que tiene por delante, a pesar del tiempo transcurrido desde el comienzo de su actuación (ya trece años), es ingente. Episodios semejantes a los descritos en relación con las administraciones públicas han tenido como protagonistas a empresas privadas, como, por ejemplo, arrojar a la basura informes elaborados sobre los aspirantes a un empleo. E incluso cabe pensar que, si entidades particulares han llegado a tratar datos sensibles sin pedir el necesario consentimiento –como los relativos a la afiliación política [STS de 25 de enero de 2006 (casación 7396/2001)] o a las creencias [STS de 17 de abril de 2007 (casación 3755/2003)]– o que no se han preocupado por dotarles de las imprescindibles medidas de seguridad, eso se debe en buena parte a que quienes protagonizan esos hechos no tienen pleno conocimiento no ya de su prohibición, sino de lo delicado del material que utilizan, aunque eso no les exima de afrontar la responsabilidad que hayan contraído con su comportamiento.

Y aquí vuelven a ser decisivas la información y la formación en protección de datos de carácter personal, así como el estímulo a la elaboración y al uso de códigos tipo, y, desde luego, la detección de las infracciones y el castigo riguroso a quienes las cometen. Tarea que ha de desarrollarse con especial energía ante la cada vez más intensa penetración de medios como Internet, la telefonía y la televisión interactiva en todas las facetas de la vida. En este sentido, lo dispuesto en el artículo 14.3 de la Directiva 2002/58 ofrece un campo de actuación que no siempre se tiene presente y que, sin embargo, posee una enorme importancia: el de la adopción de las medidas necesarias para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales. La propia Directiva 2002/58, en sus considerandos 24.º y 25.º, explica con claridad los problemas que para la protección del derecho a la autodeterminación informativa plantean los programas espías y, en general, los dispositivos ocultos que pueden introducirse en el equipo terminal del usuario y suministrar información

sobre él, extremos estos sobre los que se extiende la intervención del profesor Yves Poullet en esta misma sesión.

Problemas sobre los cuales, la Ley 32/2003, General de Telecomunicaciones, que ha transpuesto la directiva, no ha aportado soluciones.

Recientemente, el 1 de marzo del 2007, el Garante para la Protección de los Datos Personales de Italia ha aprobado una instrucción sobre *la utilización del correo electrónico e Internet en el marco de la relación de trabajo*. En ella se ocupa de sentar los criterios que han de observar los empleadores, públicos y privados, para organizar el uso que sus trabajadores hacen a través de los equipos de la empresa de esos medios de comunicación. Insiste especialmente en la protección de los datos personales de los empleados, ya sean los que puedan ser captados cuando realizan el trabajo que les corresponde, o los que tengan que ver con ellos mismos, y se detiene en los medios de control que puede disponer el empleador. En este sentido, prohíbe la lectura y el registro sistemático de los mensajes de correo electrónico o de la información sobre éstos más allá de cuanto sea técnicamente necesario para desarrollar el servicio, así como la reproducción y eventual memorización sistemática de las páginas web visualizadas por el trabajador. Igualmente, prohíbe la lectura y el registro de los caracteres introducidos desde el encabezamiento o análogo dispositivo y el análisis oculto de ordenadores portátiles puestos a su disposición.

Pues bien, éste es otro terreno en el que es preciso avanzar criterios claros por la proyección prácticamente general de la relación de empleo y porque ha suscitado problemas sobre los que no se ha llegado a establecer reglas precisas, lo que ha propiciado decisiones judiciales oscilantes.

La labor por realizar no es, ciertamente, una tarea que pueda enfocarse aisladamente desde un solo país, precisamente por la propia naturaleza de las formas de comunicación electrónica y de su capacidad para operar por encima de las fronteras. Precisamente por esa razón, la Directiva 95/46 ha erigido un sistema europeo de control que ha de ser fortalecido. Al mismo tiempo, a partir de la importante plataforma que ofrece la Unión Europea, es necesario intensificar todos los esfuerzos posibles para forjar acuerdos internacionales que extiendan las normas y las instituciones ideadas para proteger este derecho fundamental, de manera que no queden lugares vacíos de regulación en los que puedan encontrar refugio quienes pretenden aprovecharse de la información personal en beneficio propio y en desprecio del perjuicio que causan a los afectados.

6. A modo de conclusión

Nos encontramos en el comienzo de una nueva etapa. Una vez sentadas las bases constitucionales, legislativas e institucionales del derecho a la autodeterminación informativa, es menester abordar su decidida defensa con los medios jurídicos de los que ya se dispone. Es como pasar de la teoría a la práctica, de la norma a la realidad, tomando en serio los peligros que acechan y la relevancia del bien jurídico amenazado.

En ese empeño, no hay que olvidar que el derecho a la autodeterminación informativa es un derecho fundamental. Que se dirige a satisfacer una necesidad básica de toda persona: el control de la información que le concierne. Que no consiste en una exquisitez jurídica ni en un capricho, sino en una pretensión esencial en la sociedad en la que vivimos. Sin ese control, sin los límites que comporta para los poderes públicos y para los sujetos privados, ya sean los gobernantes, ya sean las empresas u otras entidades privadas, contarán no sólo con un conocimiento potencialmente pleno de la vida de cada uno de nosotros, sino que lo utilizarán para tomar decisiones que nos afectarán directa o indirectamente pero siempre de manera decisiva. El resultado será que estará en peligro el libre desenvolvimiento de nuestra vida e, incluso, nuestra propia identidad.

No es, por tanto, una cuestión menor, sino todo lo contrario. Además, el nivel de las amenazas aumenta exponencialmente a medida que se refinan –con el concurso del vertiginoso avance tecnológico– las técnicas y procedimientos que permiten acceder a datos de carácter personal y elaborarlos. Por otro lado, no hablamos de un problema específico o localizado en uno o varios países, sino que tiene una proyección universal. Ciertamente, el problema no se presenta en todos los sitios con la misma intensidad, ya que guarda relación con el grado de desarrollo de la sociedad de que se trate; sin embargo, en las sociedades que participan de los niveles de desarrollo que son propios de las nuestras, se plantea con toda su fuerza. Y, en tanto quienes no lo han alcanzado aspiran a lograrlo, también lo irán viviendo de forma creciente, con independencia de que ya les esté afectando.

Los datos de carácter personal ofrecen a quienes disponen de ellos poder y dinero. Dos estímulos ante los que es muy difícil oponer barreras eficaces si los interesados, las instituciones y los Estados no actúan de manera firme para contenerlos. El derecho a la autodeterminación informativa es un instrumento que permite luchar contra los excesos en el uso por terceros de información personal para extender su capacidad de dominación o influencia sobre los titulares de esa información u obtener beneficios económicos a su costa o gracias a ellos. Y la lucha por el derecho de la que hablaba Ihering es también y, sobre todo, lucha por los derechos. Ésta es la primera condición para que sean respetados.

La singularidad de la batalla por la autodeterminación informativa estriba en que se trata de una empresa que debe ser afrontada en la misma escala en la que operan las amenazas que se ciernen sobre ella. Solamente con actuaciones concertadas internacionalmente será posible lograr resultados eficaces frente al fenómeno de Internet, dado que no descansa en una localización determinada, sino que constituye una red con una multiplicidad de puntos desde los cuales se puede operar hacia el resto del mundo. Ya decía antes que la Unión Europea ha puesto en marcha un mecanismo de control de ámbito comunitario. Se trata de extender ese modo de operar a espacios más amplios para llevar a ellos normas y mecanismos de control que las hagan efectivas.

Es una tarea difícil porque debe tener en cuenta que no siempre se comparten los mismos criterios sobre cómo ha de asegurarse la protección de los datos de carácter personal. Se ha hablado a ese respecto de una diferente cultura en Estados Unidos y en Europa. No obstante, aun dejando un margen relevante para la iniciativa de los particulares, la autorregulación y el juego de la competencia, me parece que el esfuerzo y la responsabilidad principal debe descansar en los Estados y en sus organizaciones, ya que los Estados son los protagonistas indiscutibles de la vida internacional y siguen siendo instrumento imprescindible para la organización de la convivencia pacífica de las sociedades. Aunque parezca paradójico, los derechos necesitan de los Estados y se resienten cuando éstos son débiles.

No creo que deba plantearse una disyuntiva entre la intervención pública y la actuación privada como opciones alternativas y excluyentes. Sí pienso, en cambio, que la segunda debe ser dirigida e impulsada por la primera, ya que el mercado y la sociedad por sí mismos, no generarán espontáneamente remedios eficaces y perceptibles para todos los individuos. Sucede algo parecido a lo que se planteó, en su momento, a propósito de los derechos de los consumidores y usuarios: la lógica de la competencia no es suficiente para poner coto a las prácticas abusivas. Son, pues, necesarias regulaciones acordadas internacionalmente e instituciones del mismo carácter que velen por la actuación coordinada y coherente de las autoridades estatales encargadas de servir a modo de una primera línea de defensa especializada del derecho a la autodeterminación informativa.

Sólo contando con un marco normativo e institucional internacional con el que guarden coherencia y coordinación los propios de los Estados, será posible estimular y aprovechar las iniciativas que se mueven en el plano de la sociedad. La competencia y las buenas prácticas serán verdaderamente funcionales cuando se vean apoyadas por un ordenamiento preciso, sancionando con castigos rigurosos a sus infractores. Evitar multas y condenas es un buen acicate para buscar formas de actuación cuya observancia sea respetuosa con el derecho a la autodeterminación informativa. Sin esa referencia última, la espontaneidad y la autonomía privadas únicamente ofrecerán soluciones parciales y no siempre homogéneas, como, sin embargo, deben ser las dirigidas a hacer efectiva la protección de los datos de carácter personal.

Referencias bibliográficas

DEL CASTILLO VÁZQUEZ, Isabel Cecilia (2007). *El «habeas data»: aspectos constitucionales y administrativos (El derecho a saber y la obligación de callar)*. Tesis Doctoral. Madrid: Universidad Complutense.

FERNÁNDEZ SALMERÓN, Manuel. (2003). *La protección de datos personales en las Administraciones Públicas*. Madrid: Civitas.

LUCAS MURILLO DE LA CUEVA, Pablo (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

LUCAS MURILLO DE LA CUEVA, Pablo (1993). *Informática y protección de datos*. Madrid: Centro de Estudios Constitucionales.

LUCAS MURILLO DE LA CUEVA, Pablo (2000). «Las vicisitudes del Derecho de la protección de datos personales». *Revista Vasca de Administración Pública*. N.º 58-II. Pág. 211 y sig.

LUCAS MURILLO DE LA CUEVA, Pablo (2003). «La Constitución y el derecho a la autodeterminación informativa». Cuadernos de Derecho Público. N.º 19-20, pág. 27 y sig.

MARTÍNEZ MARTÍNEZ, Ricard (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Civitas.

TRONCOSO REIGADA, Antonio (2006). «La publicación de datos de profesores y alumnos y la privacidad personal. Acerca de la protección de datos personales en las Universidades». *Revista de Derecho Político*. N.º 67, pág. 79-163.

Cita recomendada

LUCAS MURILLO DE LA CUEVA, Pablo (2007). «Perspectivas del derecho a la autodeterminación informativa». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

‹http://www.uoc.edu/idp/5/dt/esp/lucas.pdf›

ISSN 1699-8154

Sobre el autor

Pablo Lucas Murillo de la Cueva

Magistrado del Tribunal Supremo (2001). Catedrático de Derecho Constitucional (1989). Autor, entre otras publicaciones, de los libros: *Informática y protección de datos personales* (CEC, Madrid, 1993); *El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática* (Tecnos, Madrid, 1990).

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

Hacia nuevos principios de protección de datos en un nuevo entorno TIC

Yves Poullet
con la colaboración de Jean-Marc Dinant

Fecha de presentación: mayo 2007
Fecha de aceptación: mayo 2007
Fecha de publicación: septiembre 2007

Resumen

Ante las nuevas transformaciones de Internet, entre las que podemos destacar la tendencia a la conexión de redes hasta ahora autónomas y la multifuncionalidad de los equipos terminales de telecomunicaciones, que convierten los sistemas de información en omnipresentes, hay que establecer nuevos principios para proteger adecuadamente al ciudadano.

Se proponen cinco nuevos principios. El de encriptación y anonimato reversible; el de beneficios recíprocos, de tal manera que la tecnología también beneficie a los usuarios; el de potenciación de las soluciones tecnológicas que favorezcan o no vayan en contra de la privacidad –tal como establece el Grupo del artículo 29–; el del completo control por parte del usuario del equipo terminal, de modo que éste se mantenga completamente informado de los flujos de datos, y el principio según el cual los usuarios de determinados sistemas de información se beneficien de la legislación sobre defensa de los consumidores y usuarios.

Además, la obligación de cumplimiento de las normas de protección de datos de carácter personal debe hacerse extensiva a otros sujetos que, de entrada, no parecen involucrados en el tratamiento: los fabricantes de software y de terminales. Éstos tienen el deber de informar al usuario de los riesgos que corren al utilizar las redes y de ofrecer acceso a aplicaciones y fabricar productos que garanticen una mayor protección de la privacidad.

Palabras clave

conexión de redes, nuevos principios de protección de datos, responsabilidad, fabricantes de software, fabricantes de terminales de telecomunicaciones, información al usuario

Tema

Protección de datos

Towards new Data Protection Principles in a new ICT environment

Abstract

In view of the new transformations of the Internet, among which we can highlight the trend towards previously autonomous network connections and the multifunctionality of telecommunication terminals, which make information systems omnipotent, new principles must be established in order to provide adequate protection for citizens.

Five new principles are proposed: encryption and reversible anonymity; reciprocal benefits, whereby technology also benefits users; improvement of technological solutions that favour or do not work against privacy – as established by the Group from article 29; complete user control over the terminal, so that he or she is fully informed as to the data flow; and the principle whereby users of certain information systems benefit from legislation in defence of consumers and users.

Furthermore, the obligation to comply with personal data protection regulations must be extended to other subjects that do not initially appear to be involved in processing: namely, software and terminal manufacturers. These are obliged to inform users about any risks that they run when using networks, as well as provide access to applications and manufacture products that ensure greater protection of privacy.

Keywords

networking, new data protection principles, telecommunication terminal manufacturers, information for users

Topic

Data protection

Introducción: Un nuevo entorno TIC

1. Internet y, de forma más amplia, la propagación de las TIC en nuestra vida cotidiana (GPS, RFID, móviles) han modificado radicalmente el entorno y han creado nuevos riesgos para nuestra privacidad, considerada ésta en un sentido amplio. En las dos últimas décadas se ha visto una rápida e increíble sucesión de un gran número de innovaciones y tendencias tecnológicas que han desembocado en la formación de una red de telecomunicaciones global. Este desarrollo tecnológico se ha alcanzado a nivel internacional sin que ningún gobierno o movimiento cívico jugase un papel decisivo y sin que los problemas sobre una reducción en la privacidad que acompañan a estas redes hayan sido abordados o resueltos desde el punto de vista técnico.

2. Las características de este entorno se podrían resumir como sigue y, asimismo, se sugiere determinadas metas para garantizar una mejor protección de los ciudadanos que están evolucionando más y más en «*ciudadanos de la red*».[1]

La red es **multifuncional** y tiende a enlazar todas las redes de telecomunicación existentes que hasta ahora se

1. Para una descripción completa podéis leer Y.POULLET; J.M. DINANT (nov. 2004). *Self-determination in an Information Society, Report on the application of Data Protection Principles to the worldwide Telecommunications networks*. Informe para el Comité Asesor de la Convención para la protección de individuos con respecto a procesamiento automático de Datos personales (T-PD). Estrasburgo. Disponible en la página web del Consejo de Europa. El presente artículo es una versión profundamente revisada y resumida de este informe.

mantenían autónomas. La capacidad de la infraestructura de comunicación está creciendo y se habla de que alcanzará 10 Kbits/seg.

Con respecto al **equipamiento terminal**, se observan distintas evoluciones. Primero, el equipamiento terminal, que en los ochenta era unifuncional (el terminal de telefonía de voz para transmisión de señales de audio, la TV. para la transmisión unidireccional de imágenes, etc.), ahora es **multifuncional**. Con mi portátil puedo enviar correos electrónicos, ver la TV, efectuar transacciones y leer mi periódico. Otra evolución sufrida por el equipamiento terminal es que ya no está anclada a un lugar fijo, sino que nos puede acompañar en nuestros traslados. Por otro lado, su capacidad se está incrementando de forma notable bajo la famosa Ley de Moore. Según esta teoría, cada dieciocho meses, la capacidad de un terminal puede ser doblada por el mismo precio. En otras palabras, tras quince años la capacidad de procesamiento y memoria de los ordenadores se han multiplicado por mil. En concreto, esto significa que la compra de un ordenador en un establecimiento ha sufrido la siguiente evolución:

Año	**1987**	**2005**	**2020 (x1000)**
Procesador	8 Mhertz	3 Ghertz (x 375)	3 TeraHz
Memoria	640KB	512 MB (x 800)	512 Gbytes
Disco duro	20 Mbytes	120 Gbytes (x 6000)	120 Terabytes
Conexión telefónica	10Kb/seg.	3 Mb /seg.	10 Gb/seg.

Para finalizar, también se destaca la tendencia hacia la **miniaturización** de los terminales gracias al uso de nanotecnología. Los RFID (dispositivos de identificación por radiofrecuencia) son etiquetas o tags llamadas «polvo inteligente». Estos *tags* pueden estar incrustados en nuestras ropas, en los productos que compramos en supermercados e, incluso, en nuestros cerebros y pueden detectar, controlar y, en última instancia, influir en nuestro comportamiento.

A través del uso de estos diversos terminales, los sistemas informáticos son **omnipresentes**, ya que han invadido nuestro entorno y todos los segmentos de nuestra vida cotidiana, tanto privada como profesional y, con cada día que pasa, abrirán caminos hacia nuevos campos. Los sistemas de información multiplican las huellas de los usos de los servicios TIC y asimismo multiplican la posibilidad de que determinados controladores de datos hagan un seguimiento de las actividades de los usuarios de Internet.

Muchas de las actividades, que en el pasado se llevaban a cabo sin ninguna red de telecomunicaciones, requerirán de tales redes para ser usadas en el futuro. No es descabellado pensar que, dentro de unos años, la mayoría de neveras estarán equipadas con componentes inteligentes que informarán con exactitud de qué comida está almacenada en ellas y cuándo habrán pasado sus fechas de caducidad (gracias a los chips RFID). Estas neveras «inteligentes» podrán incluso tomar la iniciativa mostrando en el televisor familiar anuncios dirigidos o contactando con los supermercados para obtener ofertas o realizando pedidos de productos. En general, existe una clara tendencia que consiste en crear objetos inteligentes a nuestro alrededor equipándolos con un terminal de telecomunicaciones. Los terminales inteligentes están operando de forma **opaca y compleja**.

3. En la actualidad, los ordenadores conforman la inmensa mayoría de terminales de telecomunicación. Al estar basados en ordenadores, estos terminales generan, de forma completamente invisible a sus usuarios, muchas huellas de las telecomunicaciones que pasan a través de ellos. Estas huellas se encuentran almacenadas en el terminal o bien se envían a través de la red, habitualmente sin informar al usuario. Los medios técnicos puestos a disposición de los usuarios son incompletos, demasiado complejos y configurados por defecto en un modo perjudicial para la protección de la privacidad de los navegantes de Internet. El respeto a la privacidad se ha convertido en una opción accesible a personas que disponen de tiempo y conocimientos. La relación del individuo con la protección de sus datos se ha convertido en sí en un artículo de información personal que muchos interesados desean poseer.

Los terminales de telecomunicación incorporan diversos identificadores técnicos que permiten «rastrear» el com-

portamiento del individuo en la red. La mayoría de participantes de la industria no consideran este proceso de rastreo una violación de la privacidad del individuo si éste no puede ser identificado mediante un punto de contacto. La tecnología de los *cookies* permite que una página web, por defecto, inserte con disimulo su propio identificador en el terminal de forma permanente para poder así rastrear el comportamiento del individuo en Internet.

4. Los protocolos de telecomunicaciones y el funcionamiento de los terminales no incluyen la protección de datos como requisito clave, sino como una opción generalmente dejada a la discreción de los fabricantes de dispositivos y programas que incorporan estos estándares. **Determinadas opiniones expresadas recientemente por el Grupo del Artículo 29 han argumentado que el principio establecido por el considerando 2 de la Directiva 95/46 UE sobre protección de datos, que afirma claramente que la tecnología debe servir en beneficio de los individuos y la sociedad, puede considerarse una justificación para imponer a los fabricantes de equipamiento terminal (incluyendo elementos de programas incorporados en los terminales) determinadas obligaciones dirigidas hacia la transparencia de su funcionamiento y prevenir el uso injusto o ilícito de datos personales asociados a la conexión y la comunicación con redes**. Se debe observar que estos fabricantes no están cubiertos como tales por la presente directiva, ya que no son los controladores de un archivo. Sin embargo, como el diseño del equipamiento que ellos proveen autoriza muchas operaciones de procesamiento, se les debería imponer determinadas responsabilidades sobre seguridad para prevenir esas operaciones que podrían realizar terceras partes de forma injusta o ilícita, y deberían ser exigibles para garantizar la transparencia, ya que el usuario del terminal debe poder ejercitar un determinado control sobre los flujos de datos generados mediante su uso.

5. Finalmente, podemos resaltar el carácter global de Internet. Debido a la naturaleza global de las redes modernas y a la ausencia de fronteras con respecto a la infraestructura, el procesamiento operado por personas localizadas fuera de las fronteras nacionales puede afectar directamente nuestra privacidad mediante el envío de spyware, transmitiendo datos a terceras partes a través de hiperenlaces invisibles o dirigiendo correo no solicitado a través de la web, etc. La abolición de fronteras nacionales hace necesaria una aproximación común hacia los principios de protección de datos y su posible imposición más allá de las fronteras. El WSIS (World Summit on the Information Society) se ha declarado a favor de un reconocimiento internacional de la protección a la privacidad.

Algunos principios nuevos para promover la autodeterminación de la información en el nuevo entorno tecnológico

6. Esos rasgos que son los más característicos del entorno del servicio de comunicaciones electrónicas –presencia creciente y multifuncionalidad de las redes y terminales de comunicación electrónica, su interactividad, el carácter internacional de las redes, servicios y productores de equipamiento y la ausencia de transparencia en el funcionamiento de terminales y redes– incrementan el riesgo de infringir las libertades individuales y la dignidad humana.

Para contrarrestar estos riesgos deben establecerse algunos nuevos principios si se desea que los interesados estén mejor protegidos y que tengan mayor control sobre su entorno. Dicho control es esencial si los usuarios van a ejercitar una responsabilidad efectiva para su propia protección y deben estar mejor preparados para ejercitar apropiadamente la autodeterminación de la información.

Éste es el primer intento de esbozo de tales principios. Está basado en una diversidad de documentación y hemos tratado de estructurarlo en torno a cinco principios clave, ya que en este estadio preferimos no hablar de nuevos «derechos» para el interesado. Su contenido y extensión debería ser discutido por otros interesados y podrían entonces, si es apropiado, formar las bases para recomendaciones y otras medidas ad hoc para dotarles de mayor fuerza.

a. Primer principio: El principio de encriptación y anonimato reversible

7. La encriptación de mensajes ofrece protección contra el acceso al contenido de las comunicaciones. La calidad varía al hacerlo las técnicas de encriptación y desencriptación. Ahora se encuentran disponibles, a precios razonables, programas de encriptación para su instalación en los ordenado-

res de los usuarios de Internet (protocolos S/MIME u Open PG). Mientras tanto, dada su ambigüedad, la noción de anonimato debería quizás ser clarificada y, posiblemente, sustituida por otros términos como «pseudoanonimato» o «no-identificable». Lo que se busca no es siempre el anonimato absoluto, sino **la no-identificación funcional del autor de un mensaje enviado a otras personas**.[2] Existen muchos documentos no vinculantes[3] defendiendo el «derecho» al anonimato de los ciudadanos cuando utilizan servicios de nueva tecnología. La recomendación núm. R (99) 5[4] del Comité de Ministros del Consejo de Europa establece que «*el acceso y uso anónimo de servicios y medios anónimos de realizar pagos son las mejores protecciones de la privacidad*», de ahí la importancia de las técnicas de potenciación de privacidad ya disponibles en el mercado.

El primer principio referido a la no identificación funcional podría ser expresado como sigue: **Aquellos que usen técnicas modernas de comunicación deben poder permanecer no identificados por los proveedores de servicios, por otras terceras partes que intervinieran durante la transmisión del mensaje y por el receptor o receptores del mensaje, y deberían tener acceso gratis, o a precios razonables, a los medios de ejercitar esta opción.**[5] **La disponibilidad de encriptación económica y herramientas y servicios para mantener el anonimato es una condición necesaria para internautas que ejerzan su responsabilidad personal**.

Sin embargo, el anonimato o la «no identificación funcional» requerida no es absoluta. El derecho del ciudadano al anonimato debe ser establecido en oposición a intereses mayores de Estado, el cual podría imponer restricciones si fuesen necesarias «*para proteger la seguridad nacional, defensa, seguridad pública, [y para] la prevención, investigación, detección y persecución de delitos*». Lograr un equilibrio entre la monitorización legítima de delitos y la protección de datos debería ser posible mediante el uso de «pseudo-identidades» que serían asignadas a individuos mediante proveedores de servicios especializados que podrían ser requeridos para revelar la identidad real de un usuario pero sólo en determinadas circunstancias y siguiendo procedimientos claramente establecidos por la ley.

8. Se podrían extraer otras consecuencias de este primer principio: podría incluir la regulación exigida de equipamientos terminales, para prevenir la monitorización de la navegación, para permitir la creación de direcciones efímeras y para la diferenciación de datos de direcciones según qué terceras partes tendrían acceso al dato de tráfico o localización, y para la desaparición de los identificadores únicos globales mediante la introducción de protocolos de direcciones uniformes.

Finalmente, el estatus de «anonimizador», en el que aquellos que lo usan depositan gran confianza, debería estar regulado para ofrecer a los afectados determinadas barreras con respecto al estándar de servicio que proporcionan, a la vez que garantizasen que el Estado posea los medios técnicos para acceder a las telecomunicaciones en circunstancias legalmente definidas.[6]

2. Véase J. GRIJPINK; C. PRIENS (2001). «Digital Anonymity on the Internet, New Rules for Anonymous Electronic Transactions?». *Computer Law & Security Report*. Vol. 17, n.º 6, pág. 379-389.
3. Véase en particular S. RODOTÀ. «Beyond the E.U. Directive: Directions for the Future». En: Y. POULLET; C. DE TERWANGNE; P. TURNER (ed.). «Privacy: New Risks and Opportunities». *Cahier du CRID*. Amberes: Kluwer. N.º 13, pág. 211 f.
4. Se encuentran disponibles varias recomendaciones para la protección de individuos con respecto a la recaudación y procesamiento de datos personales en las autopistas de la información en el sitio del Consejo de Europa. Ver también Recomendación 3/97 del llamado Grupo del Artículo 29: Anonimato en Internet, y la opinión de la comisión privada belga sobre comercio electrónico (N.º 34/2000 del 22 de noviembre de 2000, disponible en el sitio de la comisión: http://www.privacy.fgov.be), que apunta que existen tres modos de identificar los remitentes de mensajes sin que necesariamente se les requiera su identificación. .
5. Ver la recomendación de la comisión de procesamiento de datos nacionales franceses que el acceso a páginas comerciales debería ser siempre posible sin identificación previa: M. GEORGES (2000). «Relevons les défis de la protection des données à caractère personnel: l'Internet et la CNIL». *Commerce électronique-Marketing et vie privée*. París. Pág. 71 y 72.
6. Se podrían establecer los requisitos para los servicios proporcionados y con respecto a la confidenciabilidad, como se propone para las firmas digitales. La aprobación oficial de un anonimizador indicaría que se cumplen los requisitos. Tal aprobación oficial podría ser voluntaria más que obligatoria, como en el caso de etiquetas de calidad.

b. Segundo principio: El principio de beneficios recíprocos

9. Donde fuese aplicable, este principio haría que aquellos que empleen nuevas tecnologías tuviesen la obligación legal de desarrollar su actividad profesional con el fin de aceptar determinados requisitos para reestablecer el equilibrio tradicional entre las partes implicadas. La justificación es simple, si la tecnología incrementa la capacidad de acumulación, procesamiento y comunicación de información sobre terceros y facilita las transacciones y operaciones administrativas, es esencial que también esté configurada y empleada para garantizar que los interesados, tanto si son ciudadanos como consumidores, disfruten de un beneficio proporcional de estos avances.

Varias previsiones recientes se han inspirado en el requisito proporcional para obligar a que aquellos que emplean tecnologías tengan que ponerlas a disposición de los usuarios para que puedan hacer valer sus intereses y derechos.

Un ejemplo es la Directiva Europea 2001/31/CE (la «Directiva de E-Comercio»), que incluye previsiones electrónicas anti-spamming. De forma similar, el artículo 5.3 de la Directiva 2002/58/CE sobre comunicaciones privadas y electrónicas incluye, incluso, el requisito de que «...*el uso de redes de comunicación electrónicas con el fin de almacenar información u obtener acceso a la información almacenada en el equipamiento terminal de un suscriptor o usuario tan sólo está permitido bajo la condición de que al suscriptor o usuario implicado se le haya proporcionado información clara y comprensible* (...) *y se le ofrezca el derecho a rechazar dicho procesamiento* (...)». El derecho de los suscriptores, bajo el artículo 8.1, «a través de medios simples, libres de cargo alguno, eliminar la presentación de identificación de línea telefónica en términos de llamada (...) y en términos de línea» es otra aproximación potencialmente valiosa si el concepto de «línea telefónica» se amplía a diversas aplicaciones de Internet, tales como servicios web y correo electrónico.[7] Esto implica una obligación relacionada del proveedor de servicios hacia los usuarios consistente en ofrecerle las opciones de rechazar o aceptar llamadas no identificadas o prevenir su identificación (artículos 8.2 y 8.3).

10. Las legislaciones llamadas «Libertad de Información» introduce un derecho similar de transparencia con respecto al Gobierno mediante la adición de mayor información que este último tiene obligación de suministrar. Un desarrollo bien recibido en el Reino Unido es la introducción reciente de una garantía de servicio público en el manejo de datos.[8] Recientemente, una comisión sueca[9] ha recomendado una legislación que daría derechos a los ciudadanos para monitorizar sus casos electrónicamente de inicio a fin, incluyendo su archivo, y obligaría a las autoridades a adoptar una buena estructura de acceso pública, para facilitar a los individuos la identificación y localización de documentos específicos. Existe incluso un borrador de legislación que haría posible, de un modo u otro, enlazar cualquier documento oficial en el que se basasen las decisiones a otros documentos del caso. En otras palabras, un servicio público que se ha tornado más eficiente gracias a las nuevas tecnologías debe ser también más transparente y accesible para los ciudadanos. El derecho de acceso de los ciudadanos se extiende más allá de los documentos que les conciernen directamente para incluir las normativas sobre las que se basó la decisión.

11. **Es incluso posible imaginarse que determinados derechos asociados a la protección de datos, como el derecho a la información, los derechos de acceso y rectificación y el derecho a la reclamación, podrían ser de obligado cumplimiento electrónicamente. Se podrían proponer muchas aplicaciones:**

- Debería ser posible aplicar el derecho a la información de los interesados en cualquier momento mediante un

7. Obsérvese la conexión entre estas previsiones y el principio de anonimato.
8. Garantía de servicio público en el manejo de datos: disponible ahora para su implementación en entidades públicas. De este modo se establecen los derechos de las personas sobre cómo son manipulados sus datos personales y los estándares que pueden esperar que las organizaciones publicas suscriban.
http://www.dca.gov.uk/foi/sharing/psguarantees/data.htm#2
9. P. SEIPEL (2004). «Information System Quality as a Legal Concern». En: U. GASSER (ed.). *Information Quality Regulation: Foundations, Perspectives and Applications*. Nomos Verlagsgesellschaft. Pág. 248. Véase también el informe de la comisión sueca de P. SEIPEL (2002). *Law and Information Technology: Swedish Views*. Swedish Government Official Reports, SOU. Pág. 112.

simple clic (o de forma más generalizada mediante una acción electrónica e inmediata) ofreciendo el acceso a la política de privacidad, que debería ser tan detallada y completa como permita el menor coste de la propagación electrónica. Dicho paso debe ser anónimo con respecto al servidor de la página, para evitar así cualquier riesgo de creación de archivos sobre usuarios «preocupados por la privacidad». Además, en el caso de páginas a las que se han otorgado etiquetas de calidad, debería ser obligatorio que proporcionasen un hiperenlace desde el símbolo de la etiqueta hacia el organismo que le ha otorgado la etiqueta. Lo mismo sería aplicable a la declaración del controlador del archivo hacia la autoridad supervisora. Se instalaría un hiperenlace entre una página ineludible de cualquier sitio web con procesamiento de datos personales y la autoridad supervisora relevante. Finalmente, se podría prestar atención a la señalización automática de cualquier página localizada en un país que ofreciese una protección inadecuada.

- En el futuro, los interesados deberían poder ejercitar su derecho de acceso empleando una firma electrónica. Sería obligatorio estructurar los archivos para que el derecho de acceso fuese de fácil aplicación. La información adicional debería estar sistemáticamente disponible, como el origen de los documentos y un listado de los interesados a los que se les habría suministrado determinados datos. Como se ha mencionado anteriormente,[10] de forma incremental, los datos personales acumulados por un gran número de público y de redes privadas no se guardan con uno o más propósitos claramente definidos, sino que se almacenan en la red para usos posteriores que sólo emergen según surgen nuevas oportunidades de procesamiento o necesidades no identificadas previamente. En tales circunstancias, los interesados deben poder tener acceso a la documentación que describen los flujos de datos en la red, los datos concernientes y los diversos usuarios –un tipo de registro de datos.[11]
- Debería ser posible ejercitar en línea los derechos de rectificación y/o impugnación a una autoridad con un estatus claramente definido responsable de mantener o considerar un listado de quejas.
- El derecho a la reclamación debería también beneficiarse de la posibilidad de derivación en línea, intercambio de solicitudes de las partes y otras documentaciones, decisiones y proposiciones de mediación.
- Finalmente, cuando los individuos interesados deseen apelar las decisiones tomadas automáticamente o notificar mediante una red (como el rechazo a otorgar un permiso de construcción tras un llamado procedimiento e-gubernamental), deberían tener derecho a la información, mediante el mismo canal, sobre la lógica subyacente en la decisión. Por ejemplo, en el sector público[12] los ciudadanos deberían tener el derecho a probar de forma anónima cualquier paquete de toma de decisiones o sistemas expertos que pudiesen utilizar. Esto se podría aplicar a los programas para el cálculo automático de impuestos o derechos a subsidios para la rehabilitación de viviendas.

c. Tercer principio: El principio al fomento de aproximaciones tecnológicas compatibles con la situación de personas protegidas legalmente o su mejora

12. Recomendación 1/99 del llamado Grupo del Artículo 29 (grupo de trabajo sobre protección de datos de la UE),[13] que se preocupa de la amenaza a la privacidad presentada por los programas y maquinaria de comunicaciones en Internet, establece el principio de que la industria de productos de programas y maquinaria debería proporcionar las herramientas necesarias para acatar las normas europeas de protección de datos. Según este tercer principio, a

10. Ver párrafo 3.
11. Esta idea es el origen de dos leyes belgas recientes que requieren el establecimiento de comités sectoriales para las redes enlazadas al Registro Nacional (Acta del 8 de agosto de 1983 que establece un registro nacional de personas, según las amiendas del Acta del 35 de marzo de 2003, MB 28 de marzo de 2003, art. 12§1) y a la autoridad de registro comercial (Banque Carrefour des entreprises) (Acta de 16 de enero de 2003 estableciendo la autoridad, MB 5 de febrero 2003, artículo 19 §4).
12. Se aplica el mismo principio a los tomadores privados de decisiones, sujetos a los intereses legítimos de los controladores de archivo (especialmente relacionado a la confidenciabilidad de empresas, que podría limitar la obligación de clarificar la lógica subyacente).
13. Grupo del Artículo 29. Recomendación sobre el procesamiento invisible y automático de datos personales a través de Internet llevado a término mediante programas o maquinaria.

los reguladores se les debería otorgar diversos privilegios. Esta conclusión se ha deducido del considerando 2 de la Directiva 95/46 sobre protección de datos que prevé que los sistemas de información y los productos deben estar al servicio de la sociedad y de los individuos.

Por ejemplo, los reguladores deberían poder intervenir en respuesta a desarrollos tecnológicos que presente riesgos importantes. El llamado **principio de precaución**, que se encuentra bien establecido en las leyes ambientales, también podría aplicarse a la protección de datos. El principio de precaución podría requerir que el equipamiento terminal de telecomunicaciones (incluyendo los programas) adoptasen los parámetros más protectores como opción por defecto para garantizar que aquellos afectados no estén, por defecto, expuestos a los diversos riesgos de los que no tienen conocimiento y que no podrían evaluar.

De forma similar, según el principio de beneficios recíprocos, es apropiado y nada irracional equipar los terminales de telecomunicación con *weblogs* (*blogs*), como es el caso de programas tipo servidor usados por compromisos en línea y departamentos gubernamentales. Esto permitiría que los usuarios controlasen qué personas han accedido a su equipo y, cuando fuese apropiado, identificar las características principales de la información transferida.

13. Este principio puede ilustrarse con una provisión de la Directiva de la UE sobre privacidad y comunicaciones electrónicas. El artículo 14 establece que donde se requiera, la Comisión puede adoptar medidas que garanticen que el equipo terminal es compatible con las normas de protección de datos. En otras palabras, la estandarización de equipamiento terminal es otra manera, ciertamente subsidiaria, de protección de datos personales de los riesgos de procesamiento ilegal –riesgos que han sido creados por todas estas opciones de nueva tecnología. Yendo más lejos, es necesario prohibir las llamadas tecnologías para acabar con la privacidad,[14] según el principio de seguridad consagrado en el artículo 7 del Convenio 108 del Consejo de Europa. La obligación de introducir medidas técnicas y organizativas apropiadas para contrarrestar las amenazas hacia la privacidad de datos requerirá que los administradores de sitios se aseguren de que el intercambio de mensajes permanezca confidencial, y que también se indique claramente qué datos están siendo transmitidos, bien de forma automática o mediante hiperenlace, como es el caso de compañías de cibermercadotecnia.

Esta obligación de seguridad también requerirá que aquellos que procesan datos personales opten por la tecnología más apropiada para minimizar o reducir la amenaza a la privacidad. Este requisito tiene una clara influencia sobre el diseño de tarjetas inteligentes, en particular sobre tarjetas multifuncionales,[15] como las tarjetas de identificación. Otro ejemplo de la aplicación de este principio afecta a la estructura de archivos médicos a diversos niveles, como recomienda el Consejo de Europa.

14. **Se podría ir más lejos recomendando, tal y como ha hecho recientemente el Comité de la UE (2 de mayo de 2007), el desarrollo de tecnologías que potencien la privacidad, refiriéndose a herramientas o sistemas que pongan mayor énfasis en los derechos de los interesados**. Por descontado, el desarrollo de estas tecnologías dependerá del libre comportamiento del mercado, pero el Estado debe tomar una postura activa para potenciar productos que sean compatibles con la privacidad y que la cumplan, ofreciendo subsidios de investigación y desarrollo, estableciendo certificaciones voluntarias y sistemas de acreditación equivalentes, publicitando sus etiquetas de calidad y garantizando que aquellos productos que se consideren necesarios para la protección de datos estén disponibles a precios razonables.

d. Cuarto principio: El principio de que el usuario mantenga pleno control sobre el equipamiento terminal

15. La justificación para este principio es obvia. Dado que estos terminales pueden permitir que otros monitoricen nuestras acciones y comportamiento, o simplemente nos

14. Expresión utilizada por J. M. DINANT en «Law and Technology Convergence in the Data Protection Field?». En: I. WALDEN; J. HORNE (2002). *E-commerce Law and Practice in Europe*. Cambridge: Woodhead Publishers. Cap. 8.2.
15. Sobre diseños de tarjetas multi-aplicación que satisfacen la privacidad, véase E. KEULEERS; J.M. DINANT (2004). «Data protection: multi-application smart cards. The use of global unique identifiers for cross-profiling purposes». Parte 2: «Towards a privacy enhancing smart card engineering». En: *Computer Law and Security Report*. Oxford: Elsevier. Vol. 20, n.º 1, pág. 22-28.

localicen, deben funcionar de forma transparente y bajo nuestro control. El artículo 5.3 de la Directiva 2002/58/EC, citado anteriormente, ofrece una primera ilustración sobre este punto. Los interesados deben ser informados sobre cualquier acceso remoto a sus terminales mediante *cookies*, *spyware* u otros medios y deben tener la posibilidad de tomar contramedidas fáciles, efectivas y libres de cargo alguno. La Directiva 2002/58/EC también establece la norma de que los usuarios de líneas conectadas y emisores de llamadas puedan prevenir la presentación de la identificación de línea llamante.

Más allá de los anteriores ejemplos, podríamos argumentar que **todo equipo terminal debería ser configurado de forma que garantice que los propietarios y usuarios tienen información completa sobre cualquier flujo de datos entrantes o salientes para que puedan así realizar las acciones que consideren apropiadas**. De forma similar, como es ya el caso bajo determinada legislación, la posesión de una tarjeta inteligente debería estar acompañada por la posibilidad de acceder a la lectura de los datos almacenados en la tarjeta.

16. El control ejercido por el usuario también significa que los individuos pueden decidir desactivar sus terminales de forma definitiva y en cualquier momento. Esto adquiere importancia con respecto a los identificadores por radiofrecuencia (RFID). Los interesados deben tener la posibilidad de confiar en terceros[16] que garanticen que dichos medios técnicos de identificación remota han sido completamente desactivados.

Los usuarios bien podrían aplicar este principio a empresas que no se encuentran necesariamente cubiertas por las normas de protección de datos, ya que no son responsables del procesamiento de datos. Algunos ejemplos incluyen suministradores de equipo terminal y muchas formas de programas de navegación que pueden incorporarse a los terminales para facilitar la recepción, el procesamiento y la transmisión de comunicaciones electrónicas.

Este principio también se aplica a organismos de ordenación estándar públicos y privados preocupados por la configuración de dicho material y equipamiento.

17. **El punto clave radica en que los productos suministrados a los usuarios no deberían estar configurados de tal forma que pudiesen ser usados, bien por terceras partes o por los fabricantes en sí**, para propósitos ilícitos. Se puede ilustrar con varios ejemplos:

- Una comparación de los navegadores disponibles en el mercado muestra que el diálogo que intercambian sobrepasan en gran medida lo que sería estrictamente necesario para establecer la comunicación.[17]
- Entre los navegadores existe gran diversidad sobre cómo reciben, eliminan y previenen el envío de *cookies*, lo que implica que las oportunidades de procesamiento inapropiado también variarán de un navegador a otro. Sin embargo, parece ser imposible, al menos de modo simple, que en el navegador por defecto instalado en la mayoría de los cientos de millones de ordenadores personales bloquee las ventanas emergentes o la comunicación sistemática de referencias a artículos leídos en línea o a palabras clave introducidas en los motores de búsqueda.
- También se debe prestar atención al uso que hacen los suministradores de herramientas de navegación y programas de comunicación sobre identificadores únicos y *spyware*.

18. **De forma generalizada, el equipamiento terminal debería funcionar de manera transparente para que los usuarios mantuviesen un control completo sobre los datos enviados y recibidos. Por ejemplo, debería ser posible establecer, sin complicaciones, la extensión precisa del diálogo en sus ordenadores, qué archivos se han recibido, sus propósitos y quién los envió o recibió. Bajo ese punto de vista, los blogs parecen ser una herramienta apropiada que es relativamente fácil de introducir**.

19. Además del derecho del usuario a ser informado sobre los flujos de datos entrantes, existe la cuestión sobre si

16. Con certeza se refiere a acuerdos de acreditación como los descritos ya en el párrafo 15 (regulación conjunta) o la emisión, por parte de las autoridades, de autorizaciones para realizar determinadas acciones (regulación pública).
17. Ver Jean-Marc DINANT (invierno, 2001). «Le visiteur visité». *Lex Electronica*. Vol. 6, n.º 2.

las personas tienen el derecho de requerir a terceros la obtención de autorización para penetrar en su «hogar virtual». En este punto es relevante el Convenio del Consejo de Europa sobre cibercrimen, en particular los artículos 2 (acceso ilegal)[18] y 3 (intercepción ilegal).[19] En este caso, la identificación de las personas que tienen parte activa en las comunicaciones no es una precondición para la aplicación del convenio. De forma similar, el acceso no autorizado a un sistema informático no está limitado al pirateo de grandes sistemas operados por bancos o departamentos gubernamentales, sino también a accesos no autorizados a terminales de telecomunicación, estando éstos representados en la situación tecnología actual por los ordenadores.[20]

En otras palabras, mantenemos que situar un número de identificación en un terminal de telecomunicación o acceder simplemente a este número u otro identificador de terminal, constituye un acceso no autorizado. En tal contexto legal, no puede existir duda en la evaluación de proporcionalidad de dichas acciones. La autorización es un acto positivo, bastante distintivo a cualquier aceptación que pudiera ser inferida del silencio o de no expresar objeción.

Por lo tanto no se puede dar por asumido, como hizo *DoubleClick*,[21] que por el mero hecho de no activar el supresor de cookies, los usuarios hayan otorgado su autorización plena a la instalación de este tipo de información en sus terminales.

e. El principio de que los usuarios de determinados sistemas de información deberían beneficiarse de la legislación de protección al consumidor

20. **El uso rutinario de tecnologías de la información y comunicación, anteriormente confinado a actividades trascendentales, y el rápido desarrollo del comercio electrónico que ha multiplicado el número de servicios en línea han conducido a una aproximación más consumista de la privacidad**. Los navegantes de Internet ven incrementadas las transgresiones hacia su privacidad –*spamming*, creación de perfiles, políticas de cargos diferenciados, rechazo de acceso a determinados servicios, etc.– desde la perspectiva de los consumidores de estos nuevos servicios.

De este modo, en Estados Unidos los primeros pasos indecisos hacia la legislación de la protección de datos en el sector privado se enfocó en la protección del consumidor en línea. Ya se ha hecho referencia a la legislación californiana,[22] pero también deberíamos tener en cuenta la Ley de Privacidad del Consumidor de 1995 y, más recientemente, la declaración del 2000 de la Comisión de Comer-

18. Artículo 2 – Acceso ilegal: Cada parte adoptará las medidas necesarias, bien legales o de otra naturaleza, para que bajo la ley local queden establecidas como ofensas criminales el acceso a cualquier parte o a todo el sistema informático sin tener derecho, cuando se hubiesen cometido intencionalmente.
Una Parte podría requerir que la ofensa fuese cometida mediante la infracción de medidas de seguridad, con la intención de obtener datos informáticos u otra intención deshonesta, o en relación a un sistema informático conectado a otro sistema informático.
19. Artículo 3 – Acceso ilegal: Cada parte adoptará las medidas necesarias, bien legales o de otra naturaleza, para que bajo la ley local queden establecidas como ofensas criminales, cuando habiendo sido cometidas de forma intencional, la intercepción sin derecho, realizada a través de medios técnicos, de transmisiones privadas de datos informáticos, desde un sistema informático o en él, que incluyan emisiones electromagnéticas desde un sistema informático transmisor de dichos datos informáticos. Una Parte podría requerir que la ofensa fuese cometida con intención deshonesta, o en relación a un sistema informático que estuviese conectado a otro sistema informático.
20. En este contexto véase el excelente artículo de Thierry LEONARD. «E-commerce et protection des données à caractère personnel: Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet». Disponible en: http://www.droit.fundp.ac.be/Textes/Leonard1.pdf
21. A consecuencia de la demanda colectiva iniciada contra ellos hace varios años en Estados Unidos, la práctica actual de DoubleClick es enviar a todos los terminales no identificados una *cookie* inicial no residual y no identificadora llamada «aceptar cookies». Si la *cookie* es retornada, DoubleClick asume que el terminal acepta las *cookies*, y envía una *cookie* identificadora que se mantiene durante unos diez años (anteriormente treinta). Si no se retorna la *cookie*, DoubleClick enviará indefinidamente la *cookie* requiriendo autorización. Está disponible una opción de exclusión que permite a los usuarios informados almacenar una *cookie* que tiene el significado de que no las acepta.
22. Ver párrafo 12.

cio Federal,[23] que enfatiza la necesidad de legislación de privacidad para la protección de los consumidores en línea. En Europa y en América, las medidas para combatir el *spamming* se preocupan tanto de los intereses económicos de los consumidores como de los datos de privacidad de los sujetos.

21. **Esta convergencia entre los intereses económicos de los consumidores y las libertades de los ciudadanos abre perspectivas interesantes**. Sugiere que el derecho a recurrir a determinadas formas de acción colectiva, que ya están reconocidas en el campo de protección al consumidor, debería extenderse a asuntos de privacidad. Dicho derecho a «demandas colectivas» es particularmente relevante en un área en la que a menudo es difícil evaluar el perjuicio sufrido por los interesados y en el que el bajo nivel de daños concedidos es un desánimo a las acciones individuales.

Además, existen muchos aspectos de la ley del consumidor que podrían aplicarse eficazmente a la protección de datos. Algunos ejemplos serían las obligaciones de proporcionar información y asesoramiento, que podrían imponerse a los operadores que ofrecen servicios que implican esencialmente la gestión y suministro de datos personales, tales como los proveedores de acceso a Internet y servidores de bases de datos personales (bases de datos de jurisprudencia, motores de búsqueda y similares), la ley aplicable a las condiciones generales de la contratación (aplicable a política de privacidad) y medidas para combatir prácticas comerciales y competencia desleal.

Para finalizar, proporcionar datos personales como condición de acceso a un sitio web o a un servicio en línea podría ser visto no sólo bajo la perspectiva de la legislación de protección de datos –¿el consentimiento del usuario cumple los requisitos necesarios? y ¿es suficiente para legalizar el procesamiento en cuestión?– sino también bajo la legislación sobre defensa del consumidor, aunque sólo fuese en términos de prácticas injustas en la obtención de consentimiento o de obstáculos importantes surgidos del desequilibrio entre el valor de la seguridad de datos y el de los servicios suministrados.

Otro camino que hay que explorar es si la responsabilidad del producto de terminales y software puede hacerse extensiva más allá de la causación de un daño físico o económico para poder incluir la vulneración de los requisitos de protección de datos. ¿Hasta qué punto un suministrador de un navegador cuyo uso induce a vulnerar la intimidad es responsable objetivo por la violación de la normativa sobre protección de datos causada por un tercero?

Conclusiones

22. La irrupción de Internet ha creado la necesidad de una tercera generación de regulaciones sobre protección de datos. No se trata de volver la espalda a las dos primeras generaciones, sino de proporcionar un nivel adicional de protección, manteniendo inalteradas las medidas ya introducidas. La primera generación estaba principalmente basada en la naturaleza de los datos, en esencia, en si eran sensibles y si afectaban al dominio privado de los individuos. La autodeterminación informativa fue entonces equiparada con la prohibición de procesamiento de dichos datos, y se englobó en el artículo 8 de la Convención Europea de Derechos Humanos. La segunda generación se ocupaba no sólo de la protección de datos personales, sino también del modo en la que su procesamiento podría modificar el equilibrio de poder entre los procesadores de información y los sujetos de ese procesamiento. La autodeterminación informativa fue así extendida para ajustar este equilibrio mediante la garantía de que dicho procesamiento permanecería transparente y se restringiría el derecho a procesar datos sobre terceros. Éste fue el origen de la Convención N.º 108. Tiene muchos emuladores y ha justificado su existencia ampliamente.

23. **La tercera generación emergente, que esperamos se adopte con rapidez, se caracteriza por su reconocimiento de la tecnología en sí misma**. El uso de las nuevas tecnologías multiplica la cantidad de datos y de los individuos capaces de acceder a ellos, incrementa el poder de aquellos que las recopilan y procesan, y rompe

23. Ver el informe para el Congreso «Privacidad en línea: Prácticas de Información Justas» de mayo del 2000, disponible en el sitio FTC: http://www.ftc.gov/os/2000/05/index.htm. En Estados Unidos, el FTC, que es muy activo en el campo de la protección al consumidor, ha jugado un papel clave en la protección a la privacidad de los ciudadanos.

fronteras. Otro factor a tener en consideración es la complejidad y opacidad de esta tecnología. Un tercer implicado –sea el terminal o la red– interviene ahora entre el individuo y el controlador de datos. La autodeterminación informativa reclama una medida de control sobre este tercer implicado.

¿Cómo debería ejercitarse este control? Las sugerencias siguientes no son exhaustivas en el tema:

- «La respuesta a la máquina reside en la máquina» según Clarke,[24] en relación con los problemas que la sociedad de la información plantea a la propiedad intelectual. También podría sugerir vías de afrontar las amenazas que la misma sociedad presenta a la privacidad. Como ya se ha visto, el principio de beneficios recíprocos y la promoción de aproximaciones tecnológicas con «mentalidad privada» pueden ayudar a aquellos interesados en ejercitar un mayor control sobre la circulación y uso de su información personal.
- Este optimismo tiene sus límites. Aunque estas tecnologías podrían contribuir a lo que algunos llaman «empoderamiento» o «dar poder» al usuario, existe el riesgo de que a los individuos afectados se les deje hacer frente sin apoyo a los controladores de datos. En realidad, la tecnología no es neutral: aunque es ampliamente ofertada a los ciudadanos, continúa estando indirectamente financiada por las empresas y las agencias y departamentos oficiales que pagan los servidores. Inevitablemente, estos últimos están probablemente más atentos a los intereses de los controladores de datos que a los de los interesados. La llamada tecnología de protección de la privacidad transforma o podría transformar la relación entre los individuos y sus propios datos personales convirtiéndola en una relación de propiedad que, gracias a las nuevas tecnologías, se convierte en negociable. Por lo tanto es necesario destacar que la autodeterminación informativa es una libertad personal que en absoluto es susceptible de negociación y que la sociedad tiene la obligación de fijar ciertos límites al derecho de usar esos datos.
- Este enfoque sobre las herramientas tecnológicas debe también extenderse a nuevos jugadores ajenos al ámbito de la legislación de la segunda generación, principalmente a los servicios de comunicación y suministradores de equipos terminales. Su papel es crítico en cualquier intento de permitir que los usuarios de los nuevos servicios de la sociedad de la información monitoricen los datos entrantes y salientes del sistema, además de las huellas de datos que ofrecen a las redes y sus posibles usos. Se deben establecer responsabilidades estrictas en el suministro de equipamiento y servicios que cumplan con la privacidad.

24. **¿Qué quiere decir exactamente esta responsabilidad de los productores de equipos terminales y de suministros de servicios de comunicación?** En nuestra opinión, los proveedores de acceso a Internet, móviles y otros operadores telefónicos son los responsables de informar al público sobre los riegos asociados al uso de sus redes, informando sobre tecnologías amenazadoras de la privacidad y de ofrecer acceso a aplicaciones apropiadas para favorecer la privacidad. Estos proveedores de acceso tienen un papel central, ya que actúan de guardabarreras entre los usuarios y la red. Por lo tanto se les pide[25] «informar a los usuarios sobre medios técnicos que puedan usar legítimamente para reducir el riesgo para la seguridad de datos y comunicaciones», «emplear procedimientos apropiados y tecnologías disponibles, con preferencia a aquellos que han sido certificados, para proteger la privacidad de las personas afectadas (...), especialmente mediante la garantía de la integridad y confidencialidad de los datos, además de la seguridad física y lógica de la red» e informar a los usuarios de Internet sobre los modos de «usar sus servicios y pagar por ellos de forma anónima». Los suscriptores deberían tener acceso a una línea directa que les permitiese informar sobre violaciones a la privacidad, y los proveedores deberían suscribirse a un código de conducta que les obligase a bloquear el acceso a sitios web que no alcanzasen a cumplir con los requisitos de protección de datos, sin importar dónde esté localizada la página web.

24. C. CLARKE (1996). «The answer to the machine is in the machine». En: B. HUGENHOLTZ (ed.). *The Future of Copyright in a Digital Environment*. Kluwer. Pág. 139 f.
25. Recomendación del Consejo de Europa R (99) 5, III, 1, 2 y 4.

El segundo objetivo está conformado por los fabricantes y desarrolladores de equipamiento y programas, y aquellos responsables del trazado de estándares técnicos y protocolos usados en la transmisión de información de la red. Deberían garantizar que sus productos o estándares:[26]

- cumplen la ley, por ejemplo garantizando que los navegadores de Internet transmiten la información mínima necesaria para conectar y adoptar medidas de seguridad apropiadas;
- facilitan la aplicación de los principios subrayados en la parte II, por ejemplo, permitiendo a los usuarios el acceso directo a sus datos personales y al ejercicio del derecho de objeción automático, en particular mediante el uso de blogs;
- elevan el nivel de protección de datos personales.

25. Quizás, en la misma línea, debemos ampliar el alcance de la protección con respecto a los datos cubiertos por las legislaciones de privacidad. Las nuevas tecnologías hacen progresivamente posible el procesamiento de datos en relación con individuos, no, como en el caso tradicional, mediante datos relacionados a su identidad legal como el nombre o dirección, sino mediante un punto de anclaje o incluso un objeto (llamado inteligencia ambiente) asociado. Los datos generados por *cookies*, al igual que los generados por las etiquetas RFID incrustadas en la ropa o en productos, no hacen necesariamente referencia a un individuo, sino que, como permiten contactar e incluso tomar decisiones respecto de una persona, la persona tras el terminal en el caso de los *cookies* o la persona poseedora de la ropa o los productos en el caso de RFID, debe estar sujeta a determinada protección.

26. Los terminales, en el amplio sentido, deben convertirse en herramientas tecnológicas totalmente transparentes para aquellos que las tienen y las usen. Es más, en muchos casos en realidad pertenecen a los individuos interesados y podrían verse como parte de su hogar. Cualquier intrusión en su privacidad debe ser tratada como cualquier otra intrusión.

La opacidad y complejidad de los sofisticados sistemas de información a los que las personas someten datos requieren información adicional que ya no se centra estrictamente en el procesamiento en sí o en características individuales, sino en el funcionamiento general del sistema de información y su habilidad para generar una vasta cantidad de información, presente y futura. De ahí la necesidad de documentar los datos (origen, usuarios, justificación lógica), describir los diversos flujos de información y sentar normas que controlen cómo se toman las decisiones, quién tiene acceso y cómo se controla.

Hasta ahora, las autoridades de protección de datos tradicionalmente no han prestado atención a las herramientas tecnológicas. Raramente emplean especialistas informáticos o penetran en el sancta sanctorum de aquellos que deciden qué desarrollos tecnológicos se realizarán y cómo se configurarán los productos. Tal y como los Estados europeos han demandado el establecimiento de un Comité Asesor Gubernamental (GCA) al ICANN, un organismo privado responsable de la gestión de nombres y direcciones de dominios de Internet, podría ser igualmente necesario proponer o incluso insistir sobre un Comité Asesor de Protección de Datos al ICANN, W3C (Consorcio World Wide Web) y el IETF (Grupo de Trabajo en Ingeniería de Internet). Es necesario hacer que el sector de comunicaciones electrónicas sea plenamente consciente de la importancia de la protección de datos.

27. Para resumir, me gustaría destacar las dos necesidades principales siguientes:

- la necesidad de suministrar a los individuos todo lo que precisen para comprender y controlar su entorno informático; en particular, el medio de penetrar en sus hogares. Se les debe otorgar control sobre cualquier herramienta cuyo uso haga que se muestren a otros.
- la necesidad de dotar a la sociedad de herramientas para controlar los desarrollos tecnológicos, que de otro modo podrían amenazar la supervivencia de nuestras libertades colectivas e individuales.

La legislación vial impone a los usuarios determinadas normas no sólo para reducir los accidentes, sino también para alcanzar un equilibrio satisfactorio entre derechos y obligaciones de los diferentes usuarios de la carretera, estando las leyes inclinadas a ofrecer protección específica a los más vulnerables. Esto requiere no sólo un

26. Ver la opinión de la Comisión Belga n.º 34/2000 sobre comercio electrónico y protección de datos.

código vial sino legislación específica sobre la red de carreteras en sí y los vehículos que pueden usarlas, que están sujetos a determinados estándares obligatorios.

En la autopista de la información no existe una legislación que rija las normas de funcionamiento de las telecomunicaciones para la protección de la privacidad de los usuarios o requisitos para garantizar que los terminales de telecomunicación que facilitan a los usuarios navegar en esas autopistas funcionan con justicia y transparencia.

Tan sólo aplicando los principios de protección de datos tradicionales a estas nuevas tecnologías, que son implícitos pero componentes inevitables de toda telecomunicación, puede la computación dirigirnos a una sociedad de la información democrática, proporcionando progreso general para todos.

Cita recomendada

POULLET, Yves; DINANT, Jean-Marc (2007). «Hacia nuevos principios de protección de datos en un nuevo entorno TIC». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

‹http://www.uoc.edu/idp/5/dt/esp/poullet_dinant.pdf›

ISSN 1699-8154

Sobre los autores

Yves Poullet
Yves.poullet@fundp.ac.be

Profesor de la Facultad de Derecho de Namur y Lieja (Bélgica). Licenciado en Filosofía y doctor en Derecho. Director del Centre de Recherche Informatique et Droit de las Facultés Universitaires Notre-Dame de la Paix de Namur (Bélgica). Profesor de Derecho, especialmente de la enseñanza sobre «libertades y sociedad de la información», y decano de la Facultad de Derecho de las FUNDP. Asimismo, es profesor en la Universidad de Lieja.

Jean-Marc Dinant
Jean-marc.dinant@fundp.ac.be
Profesor en el *Computer Science Institute* y en el CRID (Universidad de Namur)

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

El derecho fundamental a la protección de datos: perspectivas

Ricard Martínez Martínez

Fecha de presentación: agosto de 2007
Fecha de aceptación: agosto de 2007
Fecha de publicación: septiembre de 2007

Resumen
El artículo estudia el estado actual del derecho fundamental a la protección de datos en el Ordenamiento jurídico español, y en el de la Unión Europea. Partiendo del análisis de la configuración constitucional de este derecho y de su desarrollo en el ámbito comunitario y en la legislación española, se analizan un conjunto de cuestiones relacionadas con el mismo. En primer lugar, se considera la relación del derecho fundamental a la protección de datos con el resto del ordenamiento, y en particular, los conflictos interpretativos y las colisiones con otros derechos. En todo ello se tiene muy en cuenta la realidad práctica del derecho. Por otra parte, se examina el alcance del derecho fundamental a la protección de datos y el influjo que ejerce sobre derechos conexos como el derecho a la propia imagen o el secreto de las comunicaciones. Por último, se considera el papel que debe jugar este derecho en sociedades en las que el tratamiento de información personal y las necesidades vinculadas a las políticas de seguridad ciudadana pueden afectar a las libertades de los ciudadanos.

Palabras clave
derecho fundamental a la protección de datos, vida privada, Internet, seguridad ciudadana, seguridad privada, Agencia Española de Protección de Datos

Tema
Protección de datos

The fundamental right to data protection: outlooks

Abstract
This article studies the current situation regarding the fundamental right to data protection within the Spanish legal system, as well as in the European Union as a whole. Based on an analysis of the constitutional configuration of this right and its development both in the ambit of the EU and in Spanish legislation, the article explores a series of questions related to the aforementioned right. Firstly, it considers the relationship between the fundamental right to data protection and the rest of the legal system, especially interpretative conflicts and clashes with other rights. The practical reality of this right is taken fully into account at all times. Secondly, the article examines the scope of the fundamental right to data protection, as well as its

influence on related rights such as the right to self-image and secrecy of communications. Finally, the article considers the role that this right must perform in societies where the treatment of personal information and the needs linked to citizen protection policies can affect the freedom of citizens.

Keywords
fundamental right to data protection, private life, Internet, citizen protection, private security, Spanish Data Protection Authority

Topic
Data protection

1. Consideraciones previas: la consolidación del derecho fundamental a la protección de datos

El objeto de este trabajo no es otro que realizar un breve juicio crítico sobre la historia reciente del derecho fundamental a la protección de datos apuntando elementos relevantes desde el punto de vista de la situación actual. Este derecho se ha asentado en nuestro ordenamiento con una rapidez inusitada teniendo en cuenta sus especiales características morfológicas y la técnica jurisprudencial que ha determinado su nacimiento.[1]

Como resulta sobradamente conocido –y sin perjuicio de iniciativas legislativas de muy diversa índole, cuyo objetivo era regular el uso de la informática–, el llamado derecho a la autodeterminación informativa nace en la República Federal Alemana con la sentencia dictada por el Tribunal Constitucional Federal Alemán (TCFA) en la sentencia sobre la Ley del Censo.[2] El TCFA afirma en la sentencia que el derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida. Para el TCFA:

> «la autodeterminación del individuo presupone –también en las condiciones de las técnicas modernas de tratamiento de la información– que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada.
>
> »Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación».

La consecuencia de este razonamiento es el reconocimiento jurisprudencial de un derecho fundamental a la autodeterminación informativa basado en el derecho general de la personalidad y que ofrece protección frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos de carácter personal y «garantiza la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales».[3]

1. La protección de la vida privada ha visto transcurrir un periodo de casi tres cuartos de siglo desde su primera formulación teórica por Warren y Brandeis hasta su reconocimiento jurisdiccional en Estados Unidos o para su aparición en nuestro Ordenamiento con la Constitución española de 1978. Samuel D. WARREN; Louis D. BRANDEIS (dic., 1890). «The right to privacy». *Harvard Law Review*. Vol. IV, n.º. 5.
2. Traducida por Manuel DARANAS (enero, 1984). BJC. N.º 33. Véase Manuel HEREDERO HIGUERAS (1983). «La sentencia del Tribunal Constitucional de la República Federal Alemana relativa al censo de población de 1983». *Documentación Administrativa*. N.º 198, pág. 139-158.
3. Respecto del significado de la autodeterminación informativa en la Constitución alemana, véase Antonio Enrique PÉREZ LUÑO (1989). «Libertad informática y derecho a la autodeterminación informativa». *I Congreso sobre Derecho Informático*. Facultad de Derecho de la Universidad de Zaragoza. Págs. 359-375. Y citado por Adalbert PODLECH (1984). «Art. 2 Abs. 1». *Kommentar zum Grundgesetz für die Bundesrepublik Deustchland (Reihe Alternativkommentare)*. Luchterhand, Neuwied-Darmstadt. Págs. 341 y ss.

En España la construcción doctrinal más relevante ha sido formulada por los profesores Pérez Luño[4] y Lucas Murillo de la Cueva.[5] Para el profesor Lucas Murillo, la autodeterminación informativa:

> «en cuanto que posición jurídica subjetiva correspondiente al *status de habeas data*», pretende satisfacer la necesidad, sentida por las personas en las condiciones actuales de la vida social, de preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática, y de los peligros que esto supone.
>
> »Ese objetivo se consigue por medio de lo que se denomina técnica de protección de datos, "integrada por un conjunto de derechos subjetivos, deberes, procedimientos, instituciones y reglas objetivas"».[6]

En una obra posterior, Lucas Murillo ha definido la autodeterminación informativa como:

> «el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, nuestra dignidad y libertad. En su formulación como derecho, implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito».[7]

Este planteamiento doctrinal ha sido acogido finalmente por la jurisprudencia del Tribunal Constitucional, que ha alumbrado el derecho fundamental a la protección de datos a través de un conjunto de sentencias dictadas en el periodo que va de 1993 al 2000. Debe señalarse que la primera sentencia, la número 254/1993[8] recoge el derecho, –al que denomina libertad informática–, de un modo ciertamente confuso, para después ir poco a poco perfilando el contorno del nuevo derecho.[9] Será en la STC 292/2000 donde el Alto Tribunal diseñe con nitidez el contenido del derecho fundamental a la protección de datos. El fundamento jurídico quinto de la sentencia confirma la interpretación conforme a la cual el art. 18.4 CE incorpora un nuevo derecho fundamental dotándolo de plena autonomía respecto del derecho a la intimidad:[10]

> «Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos, cuya concreta regulación debe establecer la ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio

4. PÉREZ LUÑO plantea la necesidad, en la era informática, de la existencia de un *habeas data* que se erija, del mismo modo que en su día hizo el *habeas corpus*, en cauce procesal que salvaguarde la libertad de la persona en la esfera de la informática, y entiende que el surgimiento de este derecho, que se integraría en los derechos de tercera generación, supone la necesidad de incorporar a la teoría de los estatus de Jellinek un nuevo estatus, el de *habeas data*. El autor identifica este concepto con el de «libertad informática» que define como «un nuevo derecho de autotutela de la propia identidad informática: o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico».
   A. E. PÉREZ LUÑO (1996). *Manual de informática y derecho*. Barcelona: Ariel. Pág. 43.
5. Pablo LUCAS MURILLO DE LA CUEVA (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos. Temas clave.
6. Pablo LUCAS MURILLO DE LA CUEVA (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos. Temas clave. Págs. 173-174.
7. Pablo LUCAS MURILLO DE LA CUEVA (1993). *Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)*. Cuadernos y Debates. Madrid: Centro de Estudios Constitucionales. Págs. 32 y 51. Existen posturas similares en torno a la categoría de la autodeterminación informativa. Así, puede consultarse M. HEREDERO HIGUERAS (1996). *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter Personal: comentario y textos*. Madrid: Tecnos.
8. Véase Ignacio VILLAVERDE MENENDEZ (mayo, agosto, 1994). «Protección de datos personales, derecho a ser informado, y autodeterminación informativa del individuo. A propósito de la STC 254/1993.» *Revista Española de Derecho Constitucional*. Año 14, n.º 1.
9. Véase Pablo LUCAS MURILLO DE LA CUEVA (2000). «Las vicisitudes del derecho de la protección de datos personales» en *Revista Vasca de Administración Pública*. Vol. 2, n.º 58, pág. 211-242; Pablo LUCAS MURILLO DE LA CUEVA (2003). «La primera jurisprudencia sobre el derecho a la autodeterminación informativa». *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*. N.º 1.
10. Esta interpretación se encuentra presente, ya de modo muy claro, en el conjunto de sentencias dictadas con motivo del caso RENFE sobre uso indebido de datos sobre afiliación sindical. El supuesto recogido en la sentencia, en tanto que afectaba a un colectivo de trabajadores, ha generado un conjunto de sentencias coincidentes tanto en los antecedentes como en los fundamentos jurídicos y el fallo. SSTC 11/1998, 33/1998, 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 126/1998, 158/1998, 198/1998, 223/1998, 30/1999, 44/1999 y 45/1999.

(art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».

A continuación, el fundamento jurídico sexto de la sentencia define el objeto de protección del derecho que alcanza:

«a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

En el mismo fundamento se describe el contenido del derecho fundamental a la protección de datos, que incluye un haz de garantías y facultades que se traducen en determinadas obligaciones de hacer. Se trata del derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelarlos.

Pese a que este planteamiento pueda ser criticable desde un punto de vista dogmático,[11] y tanto en lo relativo al contenido del derecho, como a la técnica empleada por el Tribunal Constitucional y a su anclaje constitucional,[12] lo cierto es que cierra de modo definitivo cualquier atisbo de debate si se tienen en cuenta distintos factores añadidos, coetáneos y posteriores a la sentencia.

El más evidente resulta de la proyección de la misma respecto del Ordenamiento español, y en particular respecto de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de los Datos de Carácter Personal, conformando un bloque normativo cuya interpretación queda claramente definida a partir de la STC 292/2000.

Junto a ello, la evolución del derecho en la Unión Europea –a pesar de la fallida Constitución o tratado constitucional– ha tomado un camino que conduce irremediablemente al reconocimiento de este derecho. En efecto, más allá de la sucesión de directivas[13] dictadas y de las constantes exigencias en esta materia contenidas por distintos convenios,[14] la Carta Europea de Derechos Fundamentales incorpora de modo expreso el derecho a la protección de datos. Con posterioridad, este derecho se incorporó al artículo II-68 de la *non nata* Constitución europea cuyo tenor literal decía:

«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

11. Véase Carlos RUIZ MIGUEL (1995). *La Configuración Constitucional del Derecho a la Intimidad*. Madrid: Tecnos.
12. Véase Ricard MARTÍNEZ MARTÍNEZ. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: APDCM-Thomson-Civitas.
13. Se han dictado distintas directivas como la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas o directiva sobre la privacidad y las comunicaciones electrónicas y la Directiva 2006/24/CE sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.
14. Así por ejemplo, puede verse el Convenio de Schengen, de 19 de junio de 1990, de aplicación del Acuerdo de Schengen de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes y el Protocolo núm. 2 por el que se integra el Acervo de Schengen en el marco de la Unión Europea. En el mismo contexto, hay que incluir el Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una Oficina Europea de Policía o Convenio Europol.

Por tanto, la línea de tendencia es clara y apunta a la consolidación de la categoría del derecho fundamental a la protección de datos. Por ello, y con independencia del juicio crítico que ello deba merecer para un jurista, nuestro primer referente debe ser siempre el derecho positivo y a su análisis se dedica este trabajo desde una perspectiva crítica y constructiva a la vez.

El conjunto de consideraciones que a continuación se exponen en relación con las perspectivas actuales del derecho fundamental a la protección de datos resultan de dos cuestiones de naturaleza diversa. En primer lugar, se pondrá de manifiesto cómo la propia definición constitucional del derecho fundamental influye de manera decisiva en el modo de actuar de los operadores jurídicos a la vez que ejerce una fuerte atracción sobre el ámbito tutelado por los derechos del artículo 18 de la Constitución española. Por otra parte, se planteará, desde un punto de vista puramente material, cómo la evolución de la realidad social y técnica sitúa a este derecho frente a un conjunto de retos ciertamente determinantes para su tutela y la de otros valores constitucionales relevantes.

2. Un derecho con perfiles muy definidos: protección de datos y conflicto de derechos

Desde el punto de vista de la concepción del derecho fundamental a la protección de datos, en nuestro sistema deben destacarse algunos elementos determinantes. En primer lugar, el Tribunal Constitucional, la Directiva 95/46/CE, y la LOPD acotan el concepto de dato personal de modo muy preciso: se trata de una información relativa a persona identificada o identificable careciendo de relevancia su naturaleza pública o privada. Pueden encontrarse elementos adicionales para establecer cuando existe un dato personal en la directiva, cuyo artículo 2 considera identificable a «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».[15] No obstante, desde el punto de vista de la aplicación de las normas sobre protección de datos, el elemento nuclear reside en un concepto determinante: el tratamiento. Sobre esta definición pivota la construcción de la Directiva 95/46/CE. El tratamiento aporta el elemento cualitativo que permite obtener información personal de un sujeto a partir de datos aparentemente irrelevantes. En este sentido, se recordará que este concepto es amplísimo, ya que, conforme al artículo 3 LOPD que transpone de modo prácticamente literal la directiva, un tratamiento abarca «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

Por tanto, cualquier actividad que pueda concebirse en relación con un dato personal constituirá un tratamiento. Como más arriba se señaló, el Tribunal Constitucional proyecta el derecho fundamental a la protección de datos sobre estos dos elementos de modo que en presencia de un dato personal la Corte advierte que, con independencia de su naturaleza pública o privada, éste puede servir para la confección de perfiles, –ideológicos, raciales, sexuales, económicos o de cualquier otra índole etc.–, subrayando que tal actividad podría constituir una amenaza para el individuo.

Por ello, los conceptos de dato y tratamiento se proyectan sobre el derecho fundamental a la protección de datos hasta conseguir cerrar una tipología muy definida. Ambos conceptos, desde el punto de vista de la aplicación de la norma ofrecen una ventaja innegable, ya que permiten emplear el mecanismo de la subsunción de modo prácticamente automático: cuando se ha identificado un dato personal que es objeto de tratamiento, el silogismo interpretativo resulta más bien

15. En la misma dirección apunta el Real Decreto 1332/1994, que en su artículo 1 define el dato de carácter personal como «toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable». Asimismo, considera que la identificación del titular de los datos podrá realizarse mediante «cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada».

sencillo y la prevalencia de lo dispuesto por la LOPD resulta prácticamente asegurada.[16]

Esta sencillez aplicativa podría estar conduciendo de hecho a una reinterpretación del conjunto del Ordenamiento jurídico en clave de protección de datos y esta técnica, aliada al ya antiguo fenómeno de la superproducción normativa, no está exenta de peligro. El problema no encuentra su origen tanto en el derecho fundamental a la protección de datos, como en el hecho de que el legislador sólo recientemente ha tenido en cuenta esta materia. Por esto, no es infrecuente que allí donde el derecho fundamental a la protección de datos debería ceder ante intereses más dignos de protección, la ley no diga absolutamente nada y ello obligue a complejos esfuerzos de interpretación normativa. La STC 292/2000, tantas veces citada, declara precisamente la inconstitucionalidad del artículo 20 LOPD en la medida en que permitía establecer comunicaciones de datos mediante disposiciones de carácter general de rango inferior a la ley. Puesto que ni antes, ni en muchas ocasiones después,[17] este hecho ha sido tenido en cuenta por el legislador. Existen ejemplos más que ilustrativos de la anterior afirmación que dan lugar a conflictos que a continuación se examinan.

2.1. Derecho de información en la recogida frente a derecho a la tutela judicial efectiva

Ni en la Ley Orgánica 15/1999 ni en las normas que regulan el ejercicio de la abogacía existe una exención del deber de información en la recogida de datos personales establecido por el artículo 5 LOPD. Por tanto, cuando un abogado proceda a la inclusión en sus ficheros de los datos de un potencial demandado proporcionados por su cliente, debería informar a éste en un plazo no superior a tres meses.[18] Sin embargo, es obvio que esta solución resulta manifiestamente inadecuada y ello ha obligado a la Agencia Española de Protección de Datos a fundamentar una excepción directamente en el derecho a la tutela judicial efectiva.[19] En tal sentido, la argumentación de la Agencia se estructura en torno a dos planteamientos. En primer lugar, la Constitución legitima el tratamiento sin consentimiento de tales datos:

> «En este caso, como se dijo, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquéllos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 del Texto Constitucional.
>
> »En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que el cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de "los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho».

A continuación, situando su argumentación en el plano del conflicto de derechos, considera que la información exigible conforme al artículo 5.4 LOPD afectaría al derecho a la tutela judicial efectiva de los demandantes:

> «Siguiendo esta premisa, en nuestra opinión debería darse una prevalencia al derecho consagrado por el artículo 24 de la Constitución, garantizando a su vez las medidas que evitarán un mayor perjuicio a los afectados (en este caso, los oponentes de los clientes cuyos datos son objeto de tratamiento).
>
> »Ello se funda en que la comunicación a los afectados de las informaciones de que los abogados o procuradores puedan disponer, procedentes de sus clientes, podrían perjudicar, como ya se indicó, el adecuado ejercicio por el propio interesado de las facultades vinculadas con su derecho a obtener la tutela efec-

16. No se pretende obviar con esta afirmación principios tan fundamentales como el del consentimiento o el de calidad de los datos y, muy particularmente, una de sus manifestaciones: la finalidad. En este sentido, el análisis de cualquier problema relacionado con la protección de datos debe tener en cuenta estos elementos. No obstante, la simple concurrencia de un dato personal y de un tratamiento pone en marcha el procedimiento interpretativo al que se alude en el texto. Sobre los principios de protección de datos, y en particular sobre la importancia del principio de finalidad véase Emilio GUICHOT (2005). *Datos personales y Administración Pública*. Madrid: APDCM-Thomson-Civitas. Pág. 230-234.
17. De hecho, el único esfuerzo coherente con lo señalado en la sentencia es el de la Ley 10/2001, de 22 de noviembre, de Cortes de Castilla-La Mancha, de adecuación de procedimientos administrativos de la Junta de Comunidades de Castilla-La Mancha y de cesión de datos personales (DOCM n.º 127 de 07/12/2001, pág. 14039).
18. En efecto el artículo 5.4 LOPD dispone: «Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad del contenido del tratamiento de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo».
19. Informe sobre tratamiento por abogados y procuradores de los datos de las partes en un proceso.

tiva de los jueces y tribunales (al quedar en conocimiento de la otra parte los datos que pudieran ser aportados a juicio en defensa de su derecho)».

En esencia, la solución aportada es la correcta y, desde un enfoque optimista, podría llevar a pensar que no existe ningún fallo en el sistema. Sin embargo, la realidad es muy distinta. El operador jurídico se encuentra ante lo que de modo un tanto exagerado podríamos denominar «un caso difícil», en el que la aplicación mecánica de la Ley Orgánica de Protección de Datos conduce a un resultado insatisfactorio. Ante la manifiesta falta de respuestas y la inactividad del legislador, se ve obligado a recurrir a elevar una consulta ante la Agencia Española de Protección de Datos. Pero ¿qué hubiera ocurrido de actuarse aplicando de modo literal lo dispuesto en la norma?

2.2. Comunicación de datos de los trabajadores frente a libertad sindical

Otro tanto sucede en el ámbito de las comunicaciones de datos personales sin consentimiento.

Un ejemplo de ello se encuentra en la sentencia dictada por el Tribunal Constitucional español en el caso COMFIA-CC.OO contra el Banco Bilbao Vizcaya Argentaria S. A. (BBVA), que constituye una interesante aproximación del Alto Tribunal a la fijación de criterios de uso de las tecnologías de la información y las comunicaciones en el ámbito laboral. En resumen, la sentencia considera que, la libertad sindical, –que se manifiesta en el caso enjuiciado en el derecho a remitir información sindical a los trabajadores–, comporta que bajo ciertas condiciones de proporcionalidad, el empresario deba soportar el envío de mensajes de correo electrónico dirigidos a las cuentas de correo corporativo asignadas a los trabajadores.[20]

Ahora bien, si el Tribunal Constitucional ha reconocido el derecho de las organizaciones sindicales a remitir a los trabajadores información sindical mediante el correo electrónico (STC 281/2005): ¿supone esto un paralelo derecho a que les sean cedidas sus direcciones electrónicas?; ¿legitimaría por tanto el ejercicio de la libertad sindical esta comunicación de datos?; teniendo en cuenta el régimen específico previsto en el artículo 7 LOPD, ¿sería necesario el consentimiento expreso de cada trabajador?[21]

Lo cierto es que, desde el punto de vista de la Ley Orgánica 15/1999, cabrían dos soluciones. La primera supone que necesariamente se exige el consentimiento expreso de cada trabajador, lo que vaciaría completamente de contenido la sentencia del Alto Tribunal. Otra posibilidad consiste en entender que cabe una comunicación de datos sin consentimiento amparada en la libertad sindical, pero con un estricto reconocimiento del derecho de oposición al tratamiento a cada destinatario de la información sindical, considerando que la alegación de la propia libertad ideológica o sindical de cada trabajador individualmente considerado constituyen los «motivos fundados y legítimos relativos a una concreta situación personal» a los que se refiere el artículo 6.4 LOPD. Ahora bien, teniendo en

20. La Corte constata el hecho de la ausencia de una obligación legal de facilitar la transmisión de información sindical a los trabajadores, afiliados o no, a través de un sistema de correo electrónico con cargo al empleador, y subraya que las empresas «no están obligadas a dotarse de esa infraestructura informática para uso sindical». Ahora bien, esto no significa a juicio del Tribunal que no exista este derecho allí donde sí existen medios informáticos. Atendido el hecho de que la difusión de información sindical forma parte del contenido esencial del derecho fundamental, el Tribunal fija distintos criterios aplicables al caso y concluye que: «sobre el empresario pesa el deber de mantener al sindicato en el goce pacífico de los instrumentos aptos para su acción sindical siempre que tales medios existan, su utilización no perjudique la finalidad para la que fueron creados por la empresa y se respeten los límites y reglas de uso que a continuación enunciaremos, cuyo cumplimiento deberá examinarse en cada caso. En tales condiciones no puede negarse la puesta a disposición, ni puede unilateralmente privarse a los sindicatos de su empleo, debiendo acudirse al auxilio judicial si con ocasión de su utilización el sindicato llega a incurrir en excesos u ocasionar perjuicios, a fin de que aquéllos sean atajados y éstos, en su caso, compensados».

21. Éste dispone:
«Artículo 7. Datos especialmente protegidos.
1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. (...)»

cuenta el efecto disuasorio del régimen sancionador de nuestra ley al que posteriormente se alude, no es muy aventurado plantearse por cuál de las dos soluciones se apostaría aplicando un mínimo de prudencia.

2.3. Derecho a la información frente a derecho fundamental a la protección de datos

En la práctica, el operador jurídico se ve abocado en multitud de ocasiones a afrontar conflictos de derechos, bienes o valores constitucionalmente relevantes y debe hacerlo con el bagaje del procedimiento de ponderación que reiteradamente ha subrayado la jurisprudencia del Tribunal Europeo de Derechos Humanos y el propio Tribunal Constitucional.[22]

Esta cuestión se agudiza muy particularmente, y tenderá a crecer, en los supuestos de ejercicio del derecho a la información y de la libertad de expresión. En efecto, los medios que la informática e Internet ponen a disposición de los individuos han minorado extraordinariamente los costes de edición de las publicaciones tradicionales. Internet pone al alcance de cualquier ciudadano la posible apertura de un blog.[23]

22. El Tribunal Europeo de Derechos Humanos ha afrontado la aplicación del artículo 8 CEDH desarrollando un método interpretativo que se articula en tres etapas de análisis netamente diferenciadas. En primer lugar, se trata de determinar si realmente se ha producido una injerencia en el derecho al respeto de la vida privada y familiar, de su domicilio o de su correspondencia, para a continuación verificar si dicha intromisión se halla prevista por ley y si es legítima y necesaria de acuerdo con las excepciones del párrafo segundo. En esta primera fase, la Corte no prejuzga en absoluto la licitud de la medida, únicamente constata si se trata o no de un supuesto que interfiere o vulnera el bien jurídico protegido por el precepto. La segunda y tercera secuencia del análisis se basan en el contraste del caso con lo dispuesto por el segundo párrafo del precepto. En primer lugar, se trata de considerar si la medida adoptada por el Estado demandado resulta amparada por el derecho. La ley además ha de ser accesible y previsible. Esto es, un ciudadano medio debería estar de algún modo en disposición de conocer la existencia de la norma o localizarla en caso de resultarle necesaria y además debería poder ajustar su conducta a las previsiones de la misma.
Una vez superado el test de legalidad, el Tribunal Europeo de Derechos Humanos finaliza su análisis emitiendo un juicio de proporcionalidad al amparo del principio de necesidad de la medida en una sociedad democrática. Véase Malone vs. the United Kingdom (1984); Carlos Ruiz Miguel (1994). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Madrid: Civitas.
La doctrina del Tribunal Constitucional al respecto de los límites a los derechos fundamentales posee un largo recorrido y arranca prácticamente con la tarea del propio Tribunal en la STC 11/1981. Muy sintéticamente expresada, la doctrina sobre las limitaciones a los derechos fundamentales exige la presencia de un fundamento constitucional de la medida, –que no puede ser otro que tratarse de un derecho o bien jurídico constitucionalizado–, cuyos límites deben estar expresamente formulados o habilitados por el constituyente, y se interpretan restrictivamente. Además, la medida limitadora debe superar un doble juicio de congruencia y proporcionalidad, ya que debe existir una mínima congruencia entre la medida restrictiva, el objetivo perseguido y el derecho limitado, y una proporcionalidad de la misma en términos de idoneidad e intervención mínima. El fundamento jurídico sexto de la STC 57/1994 sintetiza esta doctrina:
«no es ocioso recordar aquí que los derechos fundamentales reconocidos por la Constitución sólo pueden ceder ante los límites que la propia Constitución expresamente imponga, o ante los que de manera mediata o indirecta se infieran de la misma al resultar justificados por la necesidad de preservar otros derechos o bienes jurídicamente protegidos (SSTC 11/1981, fundamento jurídico 7, y 2/1982, fundamento jurídico 5, entre otras). Y tampoco que, en todo caso, las limitaciones que se establezcan no pueden obstruir el derecho fundamental más allá de lo razonable (STC 53/1986, fundamento jurídico 3). De donde se desprende que todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean necesarias para conseguir el fin perseguido (SSTC 62/1982, fundamento jurídico 5, y 13/1985, fundamento jurídico 2), ha de atender a la proporcionalidad entre el sacrificio del derecho y la situación en la que se halla aquél a quien se le impone (STC 37/1989, fundamento jurídico 7) y, en todo caso, ha de respetar su contenido esencial (SSTC 11/1981, fundamento jurídico 10; 196/1987, fundamentos jurídicos 4 a 6; 120/1990, fundamento jurídico 8, y 137/1990, fundamento jurídico 6). Por lo que ha de analizarse, a la luz de esta doctrina, si una medida como la impugnada en el presente caso se halla justificada en la protección de exigencias públicas y si, en su caso, cumple la condición de ser proporcionada en atención a la situación de aquél al que se le impone».
Véase Luis Aguiar (verano-otoño, 1983). «Dogmática y teoría jurídica de los derechos fundamentales en la interpretación de estos por el Tribunal Constitucional español». *Revista de Derecho Político*. N.º 18-19.
23. «Un blog, o en español también una bitácora, es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente. El término *blog* proviene de las palabras *web* y *log* (*log* en inglés "diario"). El término bitácora, en referencia a los antiguos cuadernos de bitácora de los barcos, se utiliza preferentemente cuando el autor escribe sobre su vida propia como si fuese un diario, pero publicado en Internet en línea».
Véase este artículo en Wikipedia http://es.wikipedia.org/wiki/Blog
En este sentido, y en la medida en el que el desarrollo de Internet en Estados Unidos ha venido anticipando problemas, no está de más recordar la sentencia dictada en el caso ACLU *vs*. Reno al señalar, en una afortunada frase, que en Internet un ciudadano tiene los mismos derechos que cualquier medio de comunicación
«Some of the dialogue on the Internet surely tests the limits of conventional discourse. Speech on the Internet can be unfiltered, unpolished, and unconventional, even emotionally charged, sexually explicit, and vulgar in a word, "indecent" in many communities. But we should expect such speech to occur in a medium in which citizens from all walks of life have a voice. We should also protect the autonomy that such a medium confers to ordinary people as well as media magnates».
United States District Court for the Eastern District Of Pennsylvania, American Civil Liberties Union, et al. *vs*. Janet Reno, Attorney General of the United States, Civil Action n.º 96-963.

Por otra parte, nada obsta en nuestro sistema para que un partido político, un sindicato o un ciudadano particular ejerzan estos derechos. Es más, en distintas ocasiones el Tribunal Constitucional ha subrayado el papel relevante que este tipo de agentes juega en la conformación de una opinión pública libre.[24]

Ahora bien, en la transposición de la Directiva 95/46/CE no se ha utilizado la habilitación que concede su artículo 9 para fijar condiciones de ejercicio de la libertad de expresión respetuosas con la intimidad.[25] Ello conduce a situaciones complejas, ya que no parece existir ninguna duda sobre la prevalencia del derecho a la información cuando, con motivo de la difusión de una información por un medio de comunicación social, exista un tratamiento de datos personales. Sin embargo, ¿qué ocurrirá cuando el ejercicio de este derecho se produzca en un boletín de información sindical o en el blog de un ciudadano?

Parece evidente que si se dan las condiciones exigibles para un correcto ejercicio del derecho a la información, éste[26] debería prevalecer. Por tanto, y en la línea apuntada tanto por el TEDH como por el Tribunal Constitucional,[27] la información debería ser relevante o de interés público y, por tanto, debería contribuir al debate público y/o a la formación de una opinión pública libre. También será relevante cuando la persona objeto de la noticia posea un carácter público y la noticia ilustre sobre algún aspecto relevante de ese perfil. Además, los hechos deberán ser veraces, aunque tal veracidad resulta entendida como diligencia en la comprobación de los mismos.

Más complejo será si cabe el conflicto cuando se trate de la libertad de expresión, cuyos requisitos de ejercicio son parcialmente diversos. Como señala la STC 160/2003, debe diferenciarse el derecho a la información de la libertad de expresión:

> «Como es sabido, nuestra jurisprudencia viene distinguiendo desde la STC 104/1986, de 17 de julio, entre los derechos que garantizan la libertad de expresión, cuyo objeto son los pensamientos, ideas y opiniones (concepto amplio que incluye las apreciaciones y los juicios de valor), y, por otra parte, el derecho a comunicar información, que se refiere a la difusión de

24. Así, en el caso de los partidos políticos la STC 48/2003 dice que el artículo 6 de la Constitución señala que los partidos políticos son «expresión del pluralismo político e instrumento fundamental para la participación política mediante su concurso a la formación y manifestación de la voluntad popular».
En segundo lugar, en la STC 136/1996 (FJ 14 y ss.) afirma el Alto Tribunal:
«14. Los derechos de participación en los asuntos públicos (art. 23.1 C.E.) y de acceso a los cargos públicos (art. 23.2 C.E.), que en la parte de su contenido que afecta a las dos vertientes del principio de representación política forman un «todo inescindible» (entre otras, SSTC 5/1983, fundamento jurídico 4, y 24/1990, fundamento jurídico 2), poseen, no sólo un contenido prestacional y una función de garantía de institutos políticos, como el de la opinión pública libre, sino también un contenido de derecho de libertad, que se concreta, en lo que aquí interesa, en la posibilidad constitucionalmente protegida de ofrecer a los ciudadanos, sin interferencias o intromisiones de los poderes públicos, los análisis de la realidad social, económica o política y las propuestas para trasformarla que consideren oportunas. (...)
15. Lo mismo puede decirse respecto de las libertades de expresión y de comunicación, cuyo contenido este Tribunal ha contribuido a perfilar en múltiples resoluciones: la primera, como el derecho fundamental del que gozan por igual todos los ciudadanos de poder expresar sus propios juicios de valor sin sufrir intromisiones por parte de los poderes públicos que no estén apoyadas en la ley, e incluso frente a la propia ley si ésta intenta fijar límites distintos a los que la Constitución admite (por todas, STC 12/1982, fundamento jurídico 3); la segunda, como la libertad de comunicar, también sin injerencias, informaciones de interés público y veraces, en el sentido de diligentemente contrastadas, sobre hechos o sobre opiniones ajenas presentadas como tales. No cabe duda de que, cuando estas libertades operan como instrumento de los derechos de participación política, debe reconocérseles, si cabe, una mayor amplitud que cuando actúan en otros contextos, ya que el bien jurídico fundamental tutelado por ellas, que es también aquí el de la formación de la opinión pública libre, adquiere un relieve muy particular en esta circunstancia, haciéndoles «especialmente resistente(s), inmune(s) a las restricciones, que es claro que en otro contexto habrían de operar» (STC 157/1996, fundamento jurídico 5, aunque se refiere a un ámbito distinto del electoral)».
25. Tratamiento de datos personales y libertad de expresión
En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados Miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.»
26. Sobre esta materia véase Lluís de CARRERAS SERRA (1996). *Régimen jurídico de la información. Periodistas y medios de comunicación*.Barcelona: Ariel; Luis ESCOBAR DE LA SERNA (1998). Derecho de la información. Madrid: Dykinson; Marc CARRILLO LÓPEZ (2003). *El derecho a no ser molestado: información y vida privada*. Pamplona: Thomson-Aranzadi.
27. Véase entre otras las SSTC 2/1988, 171/1990, 172/1990, 198/1992, 178/1993, 320/1994, 28/1996, 204/1997, 144/1998, 154/1999, 297/2000 y 76/2002.

> aquellos hechos que merecen ser considerados noticiables. Esta distinción entre pensamientos, ideas y opiniones, de un lado, y comunicación informativa de hechos, de otro, tiene decisiva importancia a la hora de determinar la legitimidad del ejercicio de esas libertades, pues mientras los hechos son susceptibles de prueba, las opiniones o juicios de valor, por su naturaleza abstracta, no se prestan a una demostración de exactitud, y ello hace que al que ejercita la libertad de expresión no le sea exigible la prueba de la verdad o diligencia en su averiguación, que condiciona, en cambio, la legitimidad del derecho de información por expreso mandato constitucional, que ha añadido al término *información*, en el texto del art. 20.1 d) CE, el adjetivo veraz (STC 4/1996, de 19 de febrero). Sin embargo, hemos admitido que en los casos reales que la vida ofrece, no siempre es fácil separar la expresión de pensamientos, ideas y opiniones de la simple narración de unos hechos, pues a menudo el mensaje sujeto a escrutinio consiste en una amalgama de ambos. Por esta razón, procede examinar en primer lugar la veracidad de aquélla y, a continuación, la ausencia de expresiones formalmente injuriosas o innecesarias para la crítica que se formula (SSTC 6/1988, de 21 de enero, 107/1988, de 8 de junio, 59/1989, de 16 de marzo, 105/1990, de 6 de junio, 171/1990, de 12 de noviembre, 172/1990, de 12 de noviembre, 190/1992, de 16 de noviembre, 123/1993, de 19 de abril, 178/1993, de 31 de mayo, 76/1995, de 22 de mayo, 138/1996, de 16 de septiembre, 204/1997, de 25 de noviembre, 1/1998, de 12 de enero), pues, como venimos diciendo, el art. 20.1 CE ni protege la divulgación de hechos que no son sino simples rumores, invenciones o insinuaciones carentes de fundamento, ni da amparo a las insidias o insultos (STC 192/1999, de 25 de octubre)».

Estamos de nuevo ante un conflicto, cuya solución parece aparentemente clara, pero que obliga a ponderar en cada ocasión los bienes en presencia.

2.4. La óptica del operador jurídico

Como se ha visto, la inexistencia de previsiones específicas obliga en muchos casos a deducir del sentido de la norma las habilitaciones para realizar determinados tratamientos. El caso paradigmático es el las comunicaciones de datos sin consentimiento del titular. Aquí la aproximación del intérprete puede realizarse reinterpretando el ordenamiento desde el punto de vista del derecho fundamental a la protección de datos con una perspectiva absolutamente garantista. Por el contrario, puede adoptarse una óptica más abierta que tenga en cuenta los intereses en juego e infiera de cláusulas generales, o de las finalidades perseguidas por la legislación, las habilitaciones necesarias para poder realizar estos tratamientos de datos sin consentimiento del titular.

Sin embargo, el aplicador cotidiano de la Ley Orgánica 15/1999 no dispone de un margen interpretativo suficiente, ya que le resulta imposible realizar este tipo de juicio por dos razones. La primera de ellas es de carácter técnico y deriva de la propia conformación del derecho fundamental a la protección de datos y de su natural prevalencia, lo que en caso de duda debe orientar la interpretación siempre a favor del derecho fundamental. Por tanto, cuando el legislador no fija con claridad la necesaria habilitación para llevar a cabo una comunicación de datos sin consentimiento, la consecuencia inmediata es la imposibilidad de realizarla.

En segundo lugar, incluso cuando el operador encuentre cierto apoyo para una comunicación de esta naturaleza, de no ser éste muy firme, –y sólo lo será si la cesión ha sido prevista expresamente por una norma con rango de ley–,[28] entra en juego un elemento disuasorio de primer orden: el régimen de infracciones y sanciones previsto por la LOPD. En efecto, el artículo 44.4.b) considera infracción muy grave «la comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas». La sanción que corresponde, en caso de tratarse de ficheros privados, puede alcanzar los seiscientos mil euros y actúa, *de facto*, como un elemento disuasorio de primer orden. En consecuencia, en caso de duda no se producirán comunicaciones de datos personales sin consentimiento, salvo cuando resulte de la emisión de informes jurídicos o del dictado de Instrucciones por la Agencia Española de Protección de Datos, o cuando la cuestión haya sido resuelta en sede judicial.

Así pues, el operador jurídico en la práctica apuesta siempre por la solución más favorable al derecho fundamental a la protección de datos, aunque un análisis sociológico seguramente arrojaría luz respecto de los factores determinantes para esta decisión. En tal sentido, a falta de un criterio empírico riguroso que avale sin genero de duda esta conclusión, lo cierto es que la lectura de las resoluciones sancionadoras permite deducir, casi a simple vista, cómo el elemento determinante no es tanto el convencimiento por parte del responsable respecto del necesario respeto del derecho fundamental, como su temor a la sanción y su deseo de minorarla.

28. Para un análisis exhaustivo de esta figura, véase Jesús Alberto MESSÍA DE LA CERDA BALLESTEROS (2003). *La cesión o comunicación de datos de carácter personal*. Madrid: Thomson-Civitas-APDCM.

Es una constante en la tramitación de procedimientos sancionadores la intención del responsable de poner en juego la previsión del artículo 45.5 LOPD que dispone:

> «Si en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquélla en que se integra la considerada en el caso de que se trate».

Para ello se acude a dos técnicas. La primera consiste en alegar «circunstancias concurrentes», y entre ellas, por lo que a este trabajo interesa, la presunción o convencimiento del ejercicio legítimo de un derecho. La segunda consiste en adoptar las medidas necesarias para cesar en el tratamiento y evitar cometer la infracción en el futuro. Lo sorprendente de esta segunda técnica es que se da no sólo en procedimientos en los que el responsable reconoce la existencia de la infracción, sino también en aquéllos en los que, existiendo un conflicto de derechos, está convencido de haber actuado correctamente y ello se aprecia claramente por la presencia de una argumentación que evidencia este convencimiento.

Un ejemplo significativo se manifiesta en el procedimiento PS/00361/2005, en el que un sindicato publicó una nota informativa en la intranet corporativa de una entidad bancaria, cuyo propósito, según las alegaciones del denunciado, era el ejercicio de la libertad sindical. No obstante, el sindicato adopta una estrategia defensiva en el sentido apuntado,[29] y lo cierto es que le rinde los beneficios esperados, ya que, como señala la resolución:

> «Durante la tramitación del presente procedimiento, ha quedado acreditado que UGT actuó en la creencia de no necesitar el consentimiento del denunciante para tratar sus datos personales y que su conducta estaba amparada por los derechos fundamentales de libertad sindical, de información y de libertad de expresión.
>
> »Igualmente, ha quedado acreditado que UGT, a través de su página web, ha dirigido una circular informativa a sus secciones sindicales para que no publiquen en Internet o intranet documentos donde se recojan datos personales si no cuentan con el consentimiento inequívoco del titular de los mismos.
>
> »En consecuencia, se considera que concurren, en el presente supuesto, circunstancias que permiten apreciar una disminución cualificada de la culpabilidad en la imputada que permite aplicar el artículo 45.5 de la LOPD».

No es aventurado cuestionarse hasta qué punto los hechos descritos generan cierta resistencia del destinatario de la norma que no alcanza a entender el cambio cultural que el derecho fundamental a la protección de datos supone, y mucho menos por qué la aplicación del mismo resulta tan severa.

3. El poder de atracción del derecho fundamental a la protección de datos

Como más arriba se señaló, un dato personal es cualquier información relativa a una persona identificada o identifica-

29. En efecto, el sindicato manifiesta que en su opinión el tratamiento efectuado respondía a «cumplir su deber de informar a los trabajadores sobre un asunto que tiene repercusión sindical. Siendo necesario valorar el hecho de que esta información viene precedida por una actuación repetida y sistemática del denunciante de hacer público a todos los empleados, a través del Lotus Notes, una serie de comunicaciones que contienen acusaciones, falsedades y calumnias de toda índole contra la Sección Sindical de UGT (...)»
En los antecedentes de hecho de la resolución, se constata como:
«Transcurrido el período de práctica de pruebas, se inició, con fecha 3 de julio de 2006, el trámite de audiencia, en el que UGT presentó escrito de alegaciones, comunicando lo siguiente:
"(...) UGT considera que los hechos denunciados no suponen la vulneración de ningún precepto de la LOPD. Ello no obstante, *ad cautelam*, en tanto no exista jurisprudencia que determine si en supuestos como el que nos ocupa prevalece el derecho a la libertad sindical, sobre el derecho a la protección de datos de carácter personal (...) o viceversa, la FES-UGT, a través del comunicado anteriormente trascrito, ha resuelto recomendar a todas sus secciones sindicales que en las circulares que publiquen por Internet o en la intranet de las empresas, se prescinda de nombre y apellidos o cualquier otro dato que pueda ser considerado de carácter personal, salvo que se tenga el consentimiento inequívoco del afectado."
Con fecha 26 de julio de 2006, UGT ha remitido copia de la circular informativa dirigida a todas las secciones sindicales de dicho sindicato, a través de su página web, en relación con la LOPD, en la que se recomienda que: "(...) en las circulares que publiquéis por Internet o en la intranet de las empresas, prescindáis de nombres y apellidos o cualquier otro dato que pueda ser considerado de carácter personal, salvo que contéis con el consentimiento inequívoco del afectado"».
Por tanto, y con independencia de sus alegaciones previas, el sindicato decidió en lo sucesivo otorgar un valor preferente al derecho fundamental a la protección de datos con independencia del juicio de prevalencia realizado sobre la libertad sindical.

ble. Por tanto, puede atribuirse la naturaleza de dato personal a una imagen, a un sonido,[30] a un número de teléfono o, como ha señalado la Agencia Española de Protección de Datos, a una dirección IP o de correo electrónico.[31] Ello apunta a un elemento cualitativo que ha puesto de manifiesto la doctrina norteamericana al utilizar el concepto de *informational privacy*.[32] Las posibilidades que ofrecen las tecnologías de la información ponen en el centro de la tutela del derecho fundamental a la protección de datos la idea de «información personal», entendida prácticamente de modo informático, como bite, como unidad que puede ser procesada por cualquier medio.

Por ello, en la práctica asistimos a un constante crecimiento del ámbito de lo protegido por el derecho fundamental a la protección de datos y, jurídicamente hablando, corremos el riesgo de invadir territorios fronterizos como el del secreto de las comunicaciones, el derecho a la propia imagen y quién sabe si en un futuro, y de la mano de la videovigilancia, el de la inviolabilidad del domicilio.[33]

En este sentido, basta con ver algunos de los temas sobre los que se ha pronunciado el Grupo de Trabajo del artículo 29, las directivas dictadas en relación con el tratamiento de datos de tráfico en las comunicaciones[34] y algunos informes jurídicos dictados por la Agencia Española de Protección de Datos[35] para verificar hasta qué punto se corre el riesgo de reducir la mayor parte del artículo 18 de la Constitución española a la idea de protección de datos. Es necesario ser conscientes de que, pese a la contundencia del aparato de tutela y sanción que ampara este derecho, ello no supone ni que la protección de datos sea la técnica más eficaz, ni la más adecuada.

30. Véase Ricard MARTÍNEZ MARTÍNEZ (2-5 de dic., 1998). «L'immagine come dato di carattere personale e la sua protezione». Convegno Internazionale: *Il diritto nella società dell'informazione*. Florencia: Istituto per la documentazione giuridica del CNR. Y (set.-dic., 2000). «Los ficheros de datos y archivos de imágenes policiales en la legislación italiana. Análisis de las resoluciones dictadas por el Garante Italiano para la protección de los datos personales». *Revista Española de Derecho Constitucional*. N.º 60.
31. Véase los informes de la Agencia Española de Protección de Datos de 1999 sobre «Tratamiento de registros de voz», «Dirección de correo electrónico» y el informe de 2003 sobre el «Carácter de dato personal de la dirección IP».
32. Véase Arthur R. MILLER (1969). «Personal privacy in the Computer Age: the challenge of a new technology and information oriented society». *Michigan Law Review*. Vol. 67; Alan F. WESTIN (1970). *Privacy and freedom* (6.ª ed.). Nueva York: Atheneum; Anita L. ALLEN (verano, 2000). «Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm». *Connecticut Law Review*. Vol. 32, pág. 861-875.
33. En este último caso debe tenerse en cuenta que, por ejemplo, con la captación de imágenes en el interior de un domicilio se produce un acto complejo en el que la entrada virtual, la propia captación de las imágenes, afectaría a la inviolabilidad del domicilio, y el registro de tales imágenes podría afectar al derecho fundamental a la protección de datos.
34. A título de ejemplo, pueden citarse entre otros documentos del Grupo de Trabajo:
    - Recomendación 2/1999, de 3 de mayo, sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones. Doc 5005/99/def. WP 18.
    - Dictamen 4/2005 sobre la propuesta de directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE (COM(2005)438 final de 21.09.2005). Doc. n.º 1868/05/ES WP 113.
    - - Dictamen 3/2006 sobre la Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, adoptada por el Consejo el 21 de febrero de 2006. Doc. n.º 654/06/ES WP 119.
35. En este ámbito, el informe más relevante probablemente sea el dictado en 1999 sobre «Solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal». La Agencia considera que el artículo 22 LOPD, en relación con el 11.2.d) de la misma norma y el 445 de la Ley Orgánica legitima para las comunicaciones de datos personales a las Fuerzas y Cuerpos de Seguridad cuando se den ciertas circunstancias:
    «a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.
    b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.
    c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.
    d) Que, en cumplimiento del artículo 22.4 de la LOPD, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento"».
    Viene a señalarse que el deber de notificación inmediata a la Autoridad Judicial o al Ministerio Fiscal del artículo 445.1 LOPJ, en relación con la comunicación prevista a favor de éstos por el artículo 11.2.d) LOPD, confirmarían esta tesis. El argumento de la Agencia, llevado al terreno de los delitos cometidos en Internet, tiene una consecuencia muy clara: una unidad policial podría requerir datos de tráfico, sin la existencia de un mandato judicial previo. Este planteamiento proporciona agilidad y contundencia a la actuación policial pero, ¿ofrece mayores garantías que las que otorga al ciudadano el derecho fundamental al secreto de las comunicaciones?

Sin embargo, la cuestión puede abordarse también desde otra perspectiva, seguramente mucho más productiva, consistente en situar el derecho fundamental a la protección de datos en el plano de la función instrumental que la Constitución, y la jurisprudencia del Tribunal Constitucional desde la STC 254/1993 le han atribuido. Por tanto, aunque en muchos de los casos en los que estén en juego los derechos del artículo 18 CE existirán tratamientos de datos personales, resultará esencial discernir tanto la realidad material de los hechos y los derechos afectados, como la técnica de tutela más adecuada.

4. El derecho fundamental a la protección de datos en una sociedad vigilada

El primer decenio del nuevo siglo está siendo claramente marcado por la idea de seguridad. No hace falta subrayar hasta qué punto está cambiando nuestro entorno tras los atentados del 11 de septiembre y el 11 de marzo. En el mundo posterior a estos atentados, el tratamiento de información personal resulta determinante para la lucha antiterrorista. Todo ello está conduciendo a una política europea integrada en esta materia en la que el Programa de La Haya del 2004 marcó una pauta clara y la directiva sobre retención de datos de tráfico en las comunicaciones constituye una primera herramienta jurídica pero no la única.

En este sentido, cabe utilizar el concepto de sociedad vigilada o sociedad control[36] si se quiere subrayar la tendencia que marca el desarrollo de la actividad del estado en esta materia. Debe recordarse hasta qué punto el informe que sobre la propuesta de la citada directiva realizaron en su día el Grupo de Trabajo del art. 29 y el Supervisor Europeo de Protección de Datos subrayaban incluso con dureza la manifiesta desproporción de algunas de las medidas que aquella contenía.[37] Por otra parte, en España se encuentra en fase de tramitación no sólo la transposición de la directiva sino también un proyecto de ley que regulará el uso de bases de datos de ADN por parte de las Fuerzas y Cuerpos de Seguridad del Estado.[38]

No obstante, el tránsito hacia una sociedad vigilada no es imputable únicamente a los actores estatales. El empleo de técnicas de control empresarial basadas en la videovigilancia, la monitorización informática e incluso la geolocalización es cada vez más frecuente. Pero no sólo en los entornos empresariales proliferan estos medios. La generalizada sensación de inseguridad a veces promovida con manifiesta irresponsabilidad por políticos y medios de comunicación, está fomentando la aparición de un creciente negocio entorno a la seguridad privada y multiplicando los controles basados en videocámaras. Éstas no siempre son regidas por expertos legitimados para ello, cualquier ciudadano puede comprar una webcam inalámbrica, enfocarla a un rellano y conectarla a un circuito de televisión.[39] Del mismo modo, la geolocalización de menores de edad es un negocio con enorme futuro.

En nuestra sociedad, son muy pocas las voces que se atreven a discutir las restricciones a las libertades que nacen con posterioridad a los atentados terroristas. Otro tanto sucede con otros procedimientos de vigilancia y control basados en la idea de seguridad privada. Parece

36. Véase David Lyon (2001). *Surveillance Society. Monitoring Everyday Life*. Open University Press, Buckingham-Philadelfia. La Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres del 1 al 3 de noviembre de 2006 ha generado un interesante documento: Lyon David Ball Kirstie; David Murakami Wood; Clive Norris; Charles Raab. *Surveillance Society' Report*. Disponible en:
‹http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance_society_report.aspx› (09/01/07).
37. Véase los documentos del Grupo de Trabajo arriba citados y el Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final].
38. En la sección de iniciativas legislativas del *website* oficial del Congreso pueden localizarse ambas:
- Proyecto de Ley Orgánica reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. BOCG. Congreso de los Diputados. Serie A, núm. 117-1, de 15 de diciembre de 2006. (Expediente núm. 121/000117.)
- Proyecto de Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación. BOCG. Congreso de los Diputados. Serie A, núm. 128-1, de 16 de marzo de 2007. (Expediente núm. 121/000128.)
39. Véase José Luis GOÑI SEIN (2007). *La videovigilancia empresarial y la protección de datos personales*. Madrid: APDC-Thomson-Civitas; Ricard MARTÍNEZ MARTÍNEZ (2007). «Videovigilancia y protección de datos personales. La Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos». *Aranzadi Revista de Derecho y Nuevas Tecnologías*. N.º 13.

evidente que la mayoría de la sociedad apuesta decidida y entusiastamente por la seguridad.

Por todo ello, la idea de la protección de datos personales como instrumento de control sobre nuestra información personal adquiere un papel fundamental en la preservación de nuestros derechos y libertades. En este contexto, el derecho fundamental a la protección de datos constituye el punto de equilibrio necesario que garantizará nuestros derechos y las autoridades de protección de datos están llamadas a jugar un papel esencial.

5. El papel determinante de las autoridades de control

En el caso español, el derecho fundamental a la protección de datos ha prosperado en un entorno normativo y jurisprudencial muy favorable pero sin que la realidad social acompañe armónicamente este desarrollo. De modo cíclico se publican noticias relativas a estudios que concluyen la existencia de un bajo grado de aplicación de la LOPD por las empresas y las administraciones españolas.[40]

Por otra parte, la mayor parte de nuestra sociedad carece de una cultura de protección de datos y ello se manifiesta de modo contundente en los procesos de captación de datos personales. Basta con comprobar hasta qué punto, ya sea en Internet o en soporte físico convencional, se tiende a actuar de modo que la prestación del consentimiento se plantee como un trámite tedioso más que el titular de los datos personales debe cumplimentar cuanto antes para llegar a su objetivo de comprar un bien o recibir un servicio. Tanto más tediosa será la técnica empleada cuanta mayor información se desee obtener.

Así, aunque en principio las normas resultan claras y sencillas de aplicar y nuestro régimen sancionador es el más exigente de Europa, podría decirse que no existe en la sociedad española una adecuada cultura de protección de datos.

Este último factor sociológico se suma a todos los elementos señalados en este trabajo para definir un escenario complejo y no necesariamente favorable a la extensión y consolidación del derecho fundamental a la protección de datos. Sin embargo, el sistema de tutela del mismo se estructura a través de autoridades independientes de control[41] y éstas están llamadas a jugar un papel determinante en la evolución del derecho fundamental a la protección de datos desde una triple perspectiva.

En primer lugar, las autoridades juegan un papel esencial desde el punto de vista de la función promocional insita en el conjunto de competencias que les atribuye la legislación sectorial. En tal sentido, las campañas de concienciación, la información al ciudadano, la generación de herramientas e instrumentos documentales, –guías, folletos etc.–, y la colaboración con otras administraciones como la municipal y/o la educativa deben acercar cada vez más al ciudadano al conocimiento del derecho fundamental a la protección de datos.

Por otra parte, debe señalarse que las autoridades de control son en la práctica intérpretes cualificados del derecho fundamental. Así, en España es común que la autoridad nacional y las autonómicas satisfagan las consultas de los ciudadanos de distintos modos, y uno de ellos consiste en elaborar informes que posteriormente son objeto de publicación. Estos documentos abarcan un amplio abanico de cuestiones y en

40. Así, en la primera conclusión de un estudio de Landwell sobre tratamiento de datos en soporte papel, éste afirma contundentemente:
«A pesar de existir una clara conciencia del riesgo que supone la ausencia de control sobre la información que genera una empresa, las empresas españolas no están en condiciones de cumplir, en la actualidad, el marco normativo que supondrá la entrada en vigor del nuevo Reglamento de la LOPD, que extenderá la obligación de aplicar medidas de seguridad a los documentos en soporte papel que contengan datos de carácter personal.»
LANDWELL PWC (2007). *Datos en papel. Tratamiento de datos personales e información confidencial en soporte papel en la empresa española*.
Asimismo, según noticias de prensa un reciente estudio de ASIMELEC (agosto-2007), afirma que sólo cumplen la LOPD un 60% de las pymes madrileñas.

41. Sobre la naturaleza y papel de las autoridades independientes, véase: Enrique GARCÍA LLOVET (1993). «Autoridades administrativas independientes y Estado de derecho». *Revista de Administración Pública*. N.º 131, págs. 61-118; Ricard MARTÍNEZ MARTÍNEZ (2001). «El control de la Agencia de Protección de Datos sobre los ficheros automatizados de datos de carácter personal de las Fuerzas y Cuerpos de Seguridad del Estado». *Cuadernos de la Cátedra Fadriqve Furió*. N.º 30-31; monográfico en homenaje al profesor Joaquín García Morillo, 2001; Artemi RALLO LLOMBARTE (2002). *La constitucionalidad de las Administraciones independientes*. Madrid: Tecnos.

muchas ocasiones son absolutamente determinantes para orientar la aplicación práctica del derecho en este sector.

Por último, debe subrayarse el papel normativo del que dispone en nuestro sistema la Agencia Española de Protección de Datos al atribuirle el artículo 37.c) LOPD competencia para dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la ley. Junto a ello, estas autoridades poseen facultades de inspección y sanción, lo cual, habida cuenta de la relevancia del régimen sancionador en España, confiere a sus resoluciones un enorme valor.

Por ello, el papel de las autoridades es determinante y esencial para la evolución del derecho fundamental a la protección de datos y debería ser ejercido desde la perspectiva de los problemas que en éste, y en otros trabajos aquí publicados, se han puesto de manifiesto.

Cita recomendada

MARTÍNEZ, Ricard (2007). «El derecho fundamental a la protección de datos: perspectivas» En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

<http://www.uoc.edu/idp/5/dt/esp/martinez.pdf>

ISSN 1699-8154

Sobre el autor

Ricard Martínez Martínez
rmartinezmarti@uoc.edu

Profesor de Derecho constitucional de la UOC. Doctor en Derecho Constitucional por la Universidad de Valencia. Premio extraordinario de doctorado. V Premio de Comunicación Científica Joan Lluís Vives de Ciencias Sociales, y de la Educación y Humanidades. Autor de tres monografías *Tecnologías de la información, policía y constitución, Una aproximación crítica a la autodeterminación informativa* y *El graduado social y la protección de datos*. Y de distintos artículos. Técnico de control de bases de datos de la Universidad de Valencia, profesor y consultor en la UOC, y participante en cursos y conferencias. Coordinador del Área de Estudios de la Agencia Española de Protección de Datos.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

La investigación policial en Internet: estructuras de cooperación internacional*

Antonio López

Fecha de presentación: mayo de 2007
Fecha de aceptación: junio de 2007
Fecha de publicación: septiembre 2007

Resumen
¿Cómo ha asumido la sociedad el fenómeno criminal en el entorno de las nuevas aplicaciones tecnológicas? ¿Cuáles son las contramedidas adoptadas por los poderes públicos sobre esta nueva realidad? El presente texto aborda ambas cuestiones tanto desde la praxis policial, cuanto desde las instituciones y foros de cooperación policial internacional, en especial los ficheros analíticos de Europol: las herramientas más sofisticadas de las que disponen las agencias de policía para la aproximación y tratamiento de esta nueva, y sin fronteras, fenomenología criminal.

Palabras clave
delincuencia informática, investigación policial, ciberinteligencia policial, cooperación policial internacional

Tema
Derecho penal y sociedad de la información

Police investigations on the Internet: structures for international cooperation

Abstract
How has society reacted to the criminal phenomenon within the area of new technological applications? What measures have been adopted by public authorities in regards to this new reality? This text addresses both questions through the police praxis as well as that of international police cooperation institutions and forums, especially the analytical files at Europol: the most sophisticated tools available to police agencies for addressing and dealing with this new, borderless criminal phenomenon.

* Texto adaptado por Jordi García Albero, profesor de los Estudios de Derecho y Ciencia Política de la UOC, a partir de la ponencia original presentada en el marco del III Congreso Internet, Derecho y Política, Barcelona, 2007.

Keywords
computer crime, police investigation, police cyber-intelligence, international police cooperation

Topic
Penal law and information society

1. Reproche penal versus reproche social. Sociedad del riesgo

Dentro de lo que genéricamente denominamos nuevas tecnologías, en especial Internet, amén de la aparición de nuevas acciones que se han reputado como penalmente típicas, (hacking, ataques DDoS,[1] etc.) y cuyo objeto es el control o la inhabilitación de una máquina dotada de un sistema informático y/o la información en ella contenida, existen multitud de viejas acciones criminales caracterizadas por nuevos *modi operandi*. Desde las injurias, calumnias y amenazas hasta las estafas; desde las infracciones contra los derechos de autor hasta la distribución de pornografía infantil; desde la apología del terrorismo hasta la negación del Holocausto. En algunos casos, estos bien conocidos delitos, evolucionados en su ejecución, no han supuesto más que un grado de sofisticación basado sobre todo en la inclusión del anonimato (tal es el caso de las injurias o amenazas); en otros, como en la pornografía infantil, la nueva dimensión que la Red les ha proporcionado ha transformado por completo su grado de peligrosidad y les ha conferido caracteres completamente novedosos.

¿Cómo ha asumido la sociedad el fenómeno criminal en este entorno de nuevas aplicaciones tecnológicas?

La respuesta requiere tomar prestado el concepto de sociedad del riesgo,[2] puesto que por él van a ser absorbidas buena parte de las amenazas ya descritas. Fenómenos como la propagación de código maligno (*viruses*) tipo gusano (no especialmente dañino), o las estafas, si lo son por una cantidad escasa, son ejemplos de acciones criminales que son asumidas por una buena parte de la población con una actitud que no suele ir más allá del mero fastidio, incluso en casos de victimación directa.[3]

1. El ataque DDoS consiste en dejar multitud de conexiones abiertas en el servidor, en espera de ser atendidas (SYN flood). El servidor reserva ciertos recursos de su sistema para atender a esas futuras conexiones, que nunca llegan a establecerse puesto que se refieren a direcciones que no existen. La máquina queda así sin recursos y deja de prestar servicio. Es como si llamáramos a una centralita telefónica y, una vez nos hubiera respondido un operador, le dijéramos «espere Ud. un momento, enseguida estoy con Ud.»; a continuación llamáramos a otro (o, más correctamente, otro socio lo hiciera desde otra línea) y repitiéramos la operación, reiterando el proceso hasta que la totalidad de los operadores quedaran con sus líneas abiertas esperando instrucciones que nunca llegarían. A las máquinas infectadas por el *malware* mencionado anteriormente se les conoce como máquinas *zombie*, y al conjunto de todas las que están a disposición de un atacante se le conoce como botnet (red de bots).
2. U. BECK(1998). *La sociedad del riesgo*. Barcelona: Paidós; M. CASTELLS (1999). *La era de la información. Economía, sociedad y cultura*. Madrid, Alianza editorial; y otros.
3. En 1999, muchos usuarios de Internet recibieron un mensaje de correo por el que se informaba de que «Gracias por haber adquirido nuestros productos. El cargo, por importe de (una cantidad entre 20.000 y 30.000 pesetas), ya ha sido procesado, y en breve será cargado en su cuenta. Si tiene alguna duda o reclamación, diríjase a nuestro departamento comercial, teléfono 90 3...». Tratándose de una compra inexistente, y siendo inminente el cargo en la cuenta bancaria, una gran mayoría de los que leyeron el mensaje se pusieron en contacto con el teléfono facilitado, que era de los de tarificación adicional y que mantenía la comunicación con la víctima hasta donde llegara su paciencia o su disponibilidad de tiempo libre. El coste de lo defraudado a cada víctima raramente llegaba a las cinco mil pesetas, cantidad que se daba por bien perdida a condición de asegurarse de que todo era una estafa y que, en realidad, nadie iba a pasar el cargo por un producto que nunca se había adquirido.

La percepción y valoración social del riesgo por parte de los responsables policiales está muy relacionada con el concepto de alarma social, fenómeno complejo, cuya evitación puede ser uno de los principales vectores de la acción policial en su conjunto.

Lo anterior merece reseñarse toda vez que, establecida una escala en cuyos extremos ubicáramos a los delincuentes que mayor y menor reproche social inspiran, ambos extremos estarían ocupados tal vez por actores propios del mundo de la «ciberdelincuencia». Así, en el extremo correspondiente al menor reproche podrían ubicarse los *piratas informáticos*,[4] mientras que a los distribuidores de pornografía infantil habría que reservar- nadie lo duda- el mayor grado de repulsa por parte del ente social.

1.1. Piratas informáticos

En la actualidad las acciones de los piratas informáticos han cambiado sustancialmente. A unas prácticas en las que los autores actuaban movidos por una suerte de inquietud intelectual por la vulnerabilidad de los sistemas informáticos, cuya calificación jurídica y posterior enjuiciamiento resultaba a veces algo comprometido si no díscolo, ha sobrevenido una realidad muy diversa: la de los denominados *hackers* al servicio de grupos de delincuencia organizada. Éstos han abandonado unos roles que en muchos casos sólo perseguían el simple reconocimiento, para ponerse a merced de grupos organizados que han sabido ver en sus habilidades un auténtico filón para explotar conjuntamente con sus estructuras criminales.

Es difícil determinar, en la actualidad, hasta qué punto ha variado la percepción social de estos *nuevos* piratas informáticos, más relacionados con las estafas y con la extorsión,[5] que con el «*hacking recreativo*».

1.2. Pornografía infantil

La persecución policial de la pornografía infantil por Internet se inició antes de que este tipo de conductas fueran criminalizadas. En efecto, con anterioridad a la modificación del Código penal sobre la materia,[6] los investigadores policiales no perseguíamos un objeto cuyo tráfico fuera ilícito (que no lo era), sino las pruebas materiales de un delito mucho más grave: la agresión sexual a menores. Y ése es el espíritu que debe continuar impulsando las actuaciones en contra de la pornografía infantil en Internet: la producción de ese material. Todo ello sin abandonar la persecución del «mero» tráfico, o incluso la tenencia de material pornográfico infantil, fundamentalmente, y en apretada síntesis, por tres poderosas razones: a) Los circuitos de pornografía infantil constituyen un monstruo que debe alimentarse constantemente con material nuevo,[7] es decir, que promueve las agresiones sexuales a menores. b) Los pedófilos son sujetos de indiscutible **interés policial**,[8] por lo que han de ser al menos

4. Por *piratas informáticos* quiere significarse un concepto vago pero muy extendido popularmente, que engloba a los *hackers*, *coders*, *crackers* (ingeniería inversa), e incluso a los que copian y distribuyen por Internet material sujeto a derechos de autor. Este término también tituló una película (1995) que contribuyó a popularizarlo y a asociarlo a las actividades características de *hacking*.
5. A finales del año 2006, agentes del Cuerpo Nacional de Policía detuvieron a un total de 23 personas entre Madrid y Cataluña, a quienes intervinieron, entre otros efectos, unas 1500 tarjetas de crédito clonadas. Las tarjetas, de una calidad nunca vista hasta entonces, incorporaban en sus bandas magnéticas los datos de entidades y ciudadanos de nacionalidad norteamericana. Estos datos habían sido almacenados en máquinas de comerciales norteamericanas que habían sido atacadas desde países del este de Europa. En este caso los *hackers* no se habían limitado a acceder al sistema y dejar pruebas de su vulnerabilidad, sino que habían obtenido los datos de las bandas magnéticas de las tarjetas de crédito, poniéndolos a disposición de la organización criminal que les contrató. Los paquetes de *dumps* – de este modo es como se conoce cada uno de los paquetes de datos magnéticos correspondiente a una tarjeta– así obtenidos son puestos en almoneda en determinados foros de Internet, o directamente explotados por éste u otro grupo criminal.
6. Operada por la Ley Orgánica 11/1999, de 30 de abril.
7. Véanse las teorías sobre la «caducidad» del poder erotógeno de la pornografía: Max TAYLOR; Ethel QUAYLE (2003). *Child pornography: an Internet crime*. Brunner-Routledge.
8. Por ejemplo, la detención de dos individuos en Barcelona y Valencia en marzo del 2007 por la **producción** de material pornográfico infantil y su distribución en Internet. Uno de ellos ya había sido detenido en el 2005 por distribución de pornografía infantil, pese a lo cual se dedicaba a «cuidar» menores en campamentos.
http://www.mir.es/DGRIS/Notas_Prensa/Policia/2007/np020402.html

identificados. c) La simple contemplación de una escena en la que aparece un menor vejado **perpetúa** la agresión contra su libertad y dignidad.

En la percepción social de este fenómeno tienen especial relevancia los medios de comunicación. Las grandes operaciones contra la pornografía infantil en Internet siempre son noticia, y los vectores que indican su importancia son invariablemente el número de detenidos y la edad mínima de los menores involucrados en las escenas. Otras consideraciones suelen ser irrelevantes. La sociedad considera peligrosa la pedofilia en sí misma, no admitiendo matices, de ahí que la repulsa social parifique conductas muy diversas: tanto da que se trate de quien elabora, quien distribuye o quien posee el material pornográfico.

La pornografía infantil no tiene su génesis en Internet, pero hay que reconocer que la red ha mutado por completo el fenómeno, haciéndolo mucho más pernicioso. La tecnología ha estado siempre especialmente unida a este tipo de agresión sexual al menor. Puede que el primer hito que le diera un nuevo impulso fuera el surgimiento de la fotografía y la cinematografía, que con toda probabilidad desplazaron al dibujo y la literatura obscenos. Las nuevas técnicas de producción de material pornográfico suponen y aportan, desde el punto de vista del consumidor, un grado de realismo hasta entonces desconocido, que trasciende a lo virtual e imaginativo.

Paralelamente, desde la óptica de la protección al menor, hay que señalar la trascendental circunstancia de que, contrariamente a lo que exige la producción de dibujo y literatura, la fotografía y la cinematografía sí requieren ineludiblemente la utilización de menores. Pero si este fue el primer hito tecnológico que revolucionó la pornografía infantil, el segundo, sin duda, ha sido Internet: **si el primero hizo inexcusable la participación del menor en la escena, el segundo ha promovido el surgimiento de la comunidad pedófila**.

En efecto, varias son las características de Internet que la configuran como un medio idóneo para los pedófilos. En primer lugar, facilita la transmisión de ficheros de un rincón a otro del Globo por un coste nimio; y, en segundo lugar, estas transacciones pueden realizarse desde identidades ficticias y de un modo más o menos anónimo, lo que indudablemente contribuye a debilitar los mecanismos de control, interiorizados o impuestos, que previenen la comisión del delito.

Pero si estos elementos son preocupantes por la mayor difusión de material pornográfico infantil que facilita la Red, lo más inquietante es que la misma posibilita la constitución de una comunidad pedófila. Así, frente a un individuo socialmente deprimido, marginado y acaso proclive a recibir terapia, emerge un *nuevo* pedófilo, miembro de una comunidad que le identifica, le refuerza y le asiste en su conducta desviada, proporcionándole no sólo el material gráfico o cualquier información necesaria para su propósito delictivo,[9] sino una razón de ser, e, incluso, la esperanza en un mundo posible en el que la pederastia tenga su cabida como una legítima opción sexual más. La publicación de argumentos y razonamientos a favor de la práctica del sexo con menores en los foros de estas comunidades se convierte en un bien tan preciado para el pedófilo como la propia pornografía infantil.

Así, el fenómeno de la pornografía infantil, considerado conjuntamente con el de las comunidades virtuales clandestinas, sí adquiere caracteres y consecuencias completamente nuevos, y requiere una consideración y tratamiento policial que necesariamente pasa por el uso de estructuras de cooperación internacional eficaces.

Paradójicamente, la proliferación de la pornografía infantil en la Red –utilizada como uno de los más poderosos argumentos por parte de los detractores de Internet– ha posibilitado la detención y posterior enjuiciamiento de agresores sexuales de menores que, en otro caso, hubieran podido permanecer ocultos mucho tiempo. Asimismo, gracias al descubrimiento y debate internacional de estas redes, muchos países han reformado sus cuerpos legales hasta ofrecer una homologada protección penal a los menores.

9. Ésta incluye desde cómo obtener sexo con menores hasta cómo prevenirse ante posibles investigaciones policiales, seguridad informática: anonimato, etc.

2. Más allá de la percepción social: la realidad de la amenaza

Un adecuado tratamiento profesional del fenómeno criminal en la Red exige conocer en qué consiste la verdadera amenaza, más allá de la mera percepción social y la alarma que pueda producir. Su determinación depende de un enfoque científico, metodológico y de ámbito internacional, que venga a determinar en forma de análisis estratégico cuáles son los elementos clave en los que deben centrarse los esfuerzos y cómo han de administrarse los recursos disponibles.

Los delitos investigados en el ámbito de Internet por las agencias policiales en todo el mundo recorren un abanico similar: pornografía infantil; fraudes (*phishing*, *pharming*, *vishing*, robos de identidad); terrorismo; tráfico de drogas (principalmente fármacos y drogas sintéticas); propiedad intelectual, etc.

¿Cuáles son las contramedidas adoptadas contra estas nuevas amenazas por los poderes públicos?

2.1. Creación de unidades de policía especializada

En 1995, el Cuerpo Nacional de Policía (CNP) creó el «Grupo de delitos informáticos» y en 1996 se estableció el «Grupo de delitos telemáticos» por parte de la Guardia Civil. Posteriormente, a medida que las policías autonómicas fueron asumiendo competencias, Mossos d'Esquadra, Ertzaina y Policía foral de Navarra crearon los suyos propios. Ubicados en sus estructuras centrales, estas unidades vienen haciéndose cargo de las investigaciones de relevancia e incluyen entre sus tareas las de asesoramiento, apoyo y/o coordinación a grupos periféricos en investigaciones de otro tipo, al menos en los casos de la Guardia Civil y el CNP. En este último, el modelo ha evolucionado con la creación de grupos especializados en su estructura periférica, con una dotación de personal, en algunos casos, de un rango similar a las unidades centrales y con una autonomía de actuación basada en el principio de subsidiariedad tan sólo limitada por una necesidad de coordinación especialmente significada[10] en las investigaciones por Internet.

Con carácter general, estas unidades policiales tienen un funcionamiento similar a las del resto de Policía Judicial;[11] si bien el resultado de su trabajo (informes, diligencias, cursos) requiere de una formación especial continua.

2.2. Establecimiento de un marco normativo adecuado

Varias son las especificidades que deben mencionarse aquí. Veamos:

a) El establecimiento de una legislación penal adecuada

El análisis de este apartado excede con mucho los propósitos de este trabajo, aunque el reconocimiento de acciones típicas entre la amplia e intrincada fenomeno-

10. La subsidiariedad constituye uno de los principios informadores de la estructura del CNP, por el que se persigue la descentralización para adaptarse a las necesidades específicas de los diversos ámbitos territoriales y lograr una mejor respuesta a las demandas de los ciudadanos. Por su parte, la coordinación, que genéricamente se refiere a las directrices de los órganos directivos superiores, a la evaluación de la actuación policial y a la inspección de los servicios, aquí tiene también un significado importante en cuanto a la competencia de la investigación dado que **los criterios de territorialidad suelen carecer de sentido en el momento de iniciarse la investigación**. De no existir herramientas eficientes de coordinación, los mismos hechos pueden ser investigados simultáneamente por varios grupos, por varios cuerpos policiales o, incluso, por varios países; y, desde luego, por varios juzgados: No conociéndose el lugar en el que se comete el hecho delictivo, resulta de aplicación el **artículo 15 de la LECr**: «*Cuando no conste el lugar en que se haya cometido una falta o delito, serán Jueces y Tribunales competentes en su caso para conocer de la causa o juicio: 1.- El del término municipal, partido o circunscripción en que se hayan descubierto pruebas materiales del delito; 2.- El del término municipal, partido o circunscripción, en que el presunto reo haya sido aprehendido; 3.- El de la residencia del reo presunto; 4.- **Cualquiera que hubiese tenido noticia del delito***». Esta cuarta opción es la que se da con mayor frecuencia. No tenemos más que imaginar que un nuevo sitio web con contenidos ilícitos es publicado en Internet, en foros de audiencia en español, y que es denunciado por cuantos usuarios se aperciben de su existencia. Tal vez convenga señalar que los gestos de sana competencia entre investigadores no debieran nunca llegar a perjudicar el resultado final de una operación, ni malgastar el erario público.
11. Con independencia de que otras unidades policiales hayan desarrollado grupos específicos para investigar en Internet las materias que les son propias, o que la Policía científica haya destinado buena parte de sus recursos a la informática forense, en la gran mayoría de los países europeos las unidades de *computer crime* se integran o asimilan a unidades de Policía judicial.

logía que Internet presenta es una de las principales tareas del investigador especializado, identificando nuevos *modi operandi*. El texto legal de referencia –El Código penal– se va modificando según las directrices de las instituciones europeas,[12] incorporando delitos nuevos o modificando los elementos de otros ya vigentes. Merece destacar la suscripción del Convenio de Cybercrime (Budapest, 23.XI.2001), por el que los países firmantes se comprometen, entre otras cosas, a incluir en su legislación penal una serie de conductas internacionalmente homologadas; base para satisfacer el principio de doble incriminación en los casos de auxilio judicial internacional.

b) La regulación administrativa del funcionamiento de los operadores de comunicaciones: en especial, el mantenimiento, conservación y tratamiento de los datos de tráfico de las mismas

La actitud de los investigadores policiales ante la retención de los datos del tráfico de las comunicaciones es fundamental, por cuanto debe entenderse que una limitación en los derechos fundamentales ha de estar debidamente justificada:

Si no existe retención de datos, no pueden investigarse los delitos en la Red.

La característica definitoria de Internet es el protocolo que le da nombre: *Internet Protocol*, siendo sus elementos individuales, las direcciones o números IP, elementos básicos de cualquier comunicación. Los **cuadernos de bitácora** en los que se registran las comunicaciones entre dos de estas direcciones son los llamados ficheros históricos o ficheros *log*. La llevanza de estos registros es automática y su conservación representa la única posibilidad de trazar *ex post facto* sucesos a nivel red. Los proveedores de servicios de Internet tienen la posibilidad de conservar unos ficheros históricos de especial relevancia: los que vinculan una dirección IP con un usuario (los que asocian la Red con el mundo real de los usuarios).

Se han defendido, sin embargo, otras actuaciones que se pretenden sustitutorias de la retención y que son mucho menos invasivas en el derecho fundamental de la privacidad, como el así denominado *quick freeze* –petición al proveedor de servicios concernido para que conserve unos determinados datos entretanto se obtiene la habilitación judicial necesaria. Esta práctica puede revelarse eficaz cuando existe un riesgo de eliminación de la información, en aquellos casos en los que, no estando regulado un periodo mínimo de conservación, puede presumirse que el proveedor va a proceder a su borrado; pero es obvio que carece de sentido si no existe un plazo de retención mínimo obligado. A mayor abundamiento, huelga sugerir el presumible comportamiento de administradores hostiles ante requerimientos tales, de no existir esta obligación general de conservación.

Se han postulado también técnicas de investigación basadas en la instalación discreta de dispositivos de *escucha*. Tales técnicas, eficaces en casos en los que existe ya un presunto autor, nada pueden aportar en el trazado *ex post facto* a nivel de red.

Como posteriormente se tratará, cualquiera de estas pesquisas policiales ha de ser habilitada judicialmente, lo que supone un trámite al que añadir el que se toma el propio proveedor de servicios para obtener y elaborar la información y respuesta, pudiéndose dilatar la averiguación de cada uno de estos escalones de trazado un plazo variable entre los diez días y varios meses, dependiendo del volumen de gestión y recursos del proveedor de servicios y la propia carga de trabajo del juzgado.

Hay otros niveles a investigar aparte del de red, pero la **comprobación de los hechos no puede obviar el enruta-**

12. Por ejemplo la DECISIÓN MARCO 2005/222/JAI DEL CONSEJO, en la que se inspira la modificación del artículo 197.3 del Código penal: «**El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo**, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años». Sin embargo, el tipo aplicable como «intrusión», con anterioridad a la reforma –artículo 197.1– incluía un elemento subjetivo que dejaba sin efecto una alta proporción de accesos no autorizados: «*El que, **para descubrir los secretos o vulnerar la intimidad de otro**, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*».

miento de las comunicaciones: Una investigación en la Red no puede prescindir del propio protocolo de Internet.

Puede argumentarse que existen técnicas y herramientas que pueden ser utilizadas por los delincuentes para obviar esta pesquisa de trazado, pero herramientas policiales como los ficheros analíticos –que más tarde se describirán– permiten ampliar enormemente el ámbito espacial y temporal de la investigación, de tal manera que habitualmente puede disponerse de un marco de referencia mucho más rico que la acción criminal propiamente dicha.

A partir de aquí corresponde a los poderes públicos evaluar la importancia de las investigaciones en Internet: hasta qué punto merece la pena menoscabar los derechos fundamentales de la privacidad y la intimidad en favor de la seguridad. El debate jurídico en el que se dilucida este asunto se sustenta en uno previo de naturaleza filosófica, social o antropológica, que afecta a la propia dialéctica de hombre individual-hombre colectivo, a la propia idea de persona, en el que todo el mundo está llamado a participar.

Personalmente, espero que los juristas sean capaces de regular con buena técnica la limitación de estos derechos fundamentales, facilitando la labor de los investigadores, la seguridad jurídica de los administradores de los proveedores de servicios, y la viabilidad comercial de sus empresas. No puedo compartir, sin embargo, el parecer de quienes identifican la retención como una práctica propia de un estado policial. Con toda honestidad, me cuesta imaginar indignación **por la retención de datos de tráfico, por un plazo de hasta doce meses, y a los que sólo se podrá acceder con habilitación judicial** cuando se analizan los hechos desde la práctica diaria y cotidiana de la limitación de los derechos. Una limitación de derechos que, en general, se admite con incomodidad (registro en el hotel; cacheos personales en el aeropuerto; revisión de bolsos y efectos personales; cámaras de vigilancia, etc.), pero que se asume e interioriza. Más bien parece que esta práctica de la retención es una mera actualización de las servidumbres que supone vivir en sociedades complejas. No faltará quien quiera ver en este incremento de las servidumbres un progresivo detrimento de los derechos individuales o de las libertades públicas, de tal manera que hoy preventivamente se guardan datos impregnados de intimidad que no se guardaban antes. Pero lo justo no es acumular un listado de cargos absolutos contra los estados e instituciones públicas, sino entenderlos en términos relativos o porcentuales, pues si bien la conservación de estas muestras impregnadas de intimidad representan una limitación en la privacidad de las personas, más cierto es que los miembros de estas sociedades modernas y desarrolladas hemos mejorado extraordinariamente las posibilidades de expresión y comunicación, así como la protección del individuo frente a los poderes públicos y la sociedad en general.

c) El carácter internacional *per se* de las acciones criminales llevadas a cabo a través de Internet

Todos los delitos relacionados con el crimen organizado tienen cierta proyección internacional. Las instituciones de cooperación policial internacional son cada vez más activas, sobre todo en el ámbito europeo, promoviendo foros de cooperación tanto a nivel estratégico como operativo. De tal proyección participan también los delitos cometidos a través de Internet, incluso más acusada, debido a su rápida evolución; pero al mencionar su carácter *per se* quiere significarse que no existe una diferencia esencial entre el uso de una máquina en Austria de una en Australia, es decir, que no existe ningún factor local de gran relevancia (salvo el del idioma). Así, el terreno de juego es el mundo entero, desvirtuando, en cierto modo, el principio de territorialidad del Derecho.

Siendo ésta una circunstancia de la mayor relevancia, su dimensión se hace más significativa si se tiene en cuenta su concurrencia con otra: la necesaria habilitación judicial desde las primeras fases de la investigación.

Metodológicamente, puede hablarse de una fase virtual de la investigación, que es la que conduciría hasta la máquina de la que partieron los hechos que la motivan. Esta fase muy pronto conduce hasta una dirección IP que, permítase la licencia de esta comparación, viene a ser la matrícula del vehículo desde el que supuestamente se ha cometido el hecho objeto de investigación. En este símil, la red pública de carreteras sería, naturalmente, Internet. Preguntémonos por las posibilidades a la hora de hacer uso de la misma con un vehículo:

- de nuestra propiedad;
- cuyo uso nos cede y asigna nuestra empresa;
- alquilado;
- taxi;
- robado;

- de un amigo;
- con placas robadas o falsas.[13]

Un vehículo de nuestra propiedad sería el equivalente a un acceso con IP contratada directamente por nosotros, adquiriendo el mismo rango que un proveedor de servicios. Si esta placa de matrícula es identificada en la comisión de una infracción, tan sólo ha de consultarse la base de datos de la Dirección General de Tráfico (DGT)[14] –o su equivalente en otro país– para saber quién es el propietario del vehículo y, en primera instancia, el infractor. Si accedemos con el vehículo que nuestra empresa nos ha asignado, nuestra IP será fija; pero en la base de datos de la DGT no constaremos como propietarios, sino nuestra empresa, que será la que tendrá que identificarnos ante la autoridad cuando para ello sea requerida: se corresponde con el caso –en nuestra comparación– de las IP fijas facilitadas por servicios ADSL. Si accedemos con un vehículo alquilado, estaríamos en el símil de acceso a través de una IP dinámica, típicamente un acceso telefónico o «dial-up», ya casi en desuso; o las que facilitan los proveedores de servicios de *cable* o, en general, los que utilicen servidores DHCP,[15] uno de los más extendidos. En este caso, un intermediario –el proveedor de servicios de Internet– ha adquirido un paquete de direcciones IP, que distribuye entre sus clientes, como la compañía de alquiler ha adquirido sus vehículos para alquilarlos entre sus clientes. La consulta a la base de datos de la DGT nos llevaría a la concreta compañía de alquiler de vehículos, que es la que consta como propietaria, y será necesario que ésta, a su vez, consulte en sus registros (en el símil estaríamos hablando de los registros de tráfico objeto de **retención**) para determinar a qué cliente concreto cedió un determinado vehículo en un determinado período de tiempo.

En el supuesto del taxi, se debería corresponder con un locutorio público o «cibercafé» dado que el taxista no registra la identidad del usuario de su servicio siendo –a los efectos que nos ocupan– el auténtico conductor del mismo, ya que es quien determina el destino (como tampoco el dueño del locutorio público registra a los clientes).

En el ejemplo del vehículo robado, en la actualidad se situaría en los accesos compartidos a Internet, típicamente corporativos, en los que tras identificarse ante el sistema con nombre de usuario y contraseña, se accede a la Red a través de un proxy: la averiguación del nombre de usuario y contraseña de otra persona y el uso del terminal usurpando sus credenciales, o el aprovechamiento de un descuido para controlar el ordenador con su conexión,[16] sería una casuística típica. Mucha más incidencia tiene, sin embargo, la interferencia de la señal de una red inalámbrica y su acceso a ella sin el conocimiento ni consentimiento de su legítimo titular.

Por otra parte, si la forma en la que accedemos a Internet fuera desde una conexión inalámbrica deliberadamente abierta (o con credenciales otorgados por su administrador), o si lo fuera desde una red corporativa haciendo uso de las credenciales de alguien que nos las cede voluntariamente, o de alguien que nos permite el uso de su equipo desde su propio domicilio, estaríamos en la correspondencia con el uso del vehículo de un amigo.

Por último, la última de las posibilidades que hemos relacionado, el acceso con un vehículo con una placa robada o falsa, se operaría mediante el uso de un troyano instalado subrepticiamente en la máquina de otro usuario, o del uso de un «proxy» para el que no estamos autorizados.

Pues bien, con excepción del primer caso, que no es más que una mera posibilidad teórica, en todos los demás es necesaria la habilitación judicial para obtener datos sobre el propietario del vehículo desde el que presuntamente se ha cometido el crimen.

Es decir, según este símil, lo que en el mundo real bastaría con una simple e inmediata consulta a la DGT, en las

13. En este caso, el símil contiene ciertas limitaciones: si bien a la red pública de carreteras se puede acceder TAMBIÉN con un vehículo sin placas, el acceso a Internet no es posible –por definición– sin una dirección IP.
14. En nuestro ejemplo, la base de datos de la DGT se corresponde con las de carácter público y abierto que relacionan rangos de IP con los proveedores de servicios que los gestionan: ARIN – Norte América www.arin.net; AfriNIC – África www.afrinic.net; APNIC – Asia – Pacífico www.apnic.net; LACNIC – América latina www.lacnic.net; RIPE - Europa, Medio oriente y Asia central www.ripe.net.
15. Dynamic Host Configuration Protocol.
16. Por ejemplo, ausentarse del lugar donde se halla el ordenador dejando la terminal sin bloquear.

investigaciones por Internet requiere necesariamente la previa obtención de un mandamiento judicial.[17]

La intervención judicial no se agota aquí, sino que se extiende a momentos posteriores en la investigación policial, siendo la más significativa, la entrada y registro en domicilio o lugar cerrado al objeto de la intervención y posterior análisis de los ordenadores desde los que se han cometido los hechos motivo de investigación. Éstas constituyen diligencias ineludibles,[18] cuya práctica, para que no quede desvirtuada, debe llevarse a cabo sin la prevención del presunto autor de los hechos. Así, el juez instructor debe decidir la proporcionalidad o desproporción entre la gravedad de los hechos investigados y la limitación de derechos solicitada: la entrada y registro en domicilio.[19]

En definitiva, puede concluirse que, desde los primeros estadios de la investigación, ésta debe ser tutelada por la autoridad judicial, habilitando la actuación de los policías mediante auto motivado en sucesivas ocasiones,[20] lo que seguiría siendo un problema asequible si el ámbito territorial se mantuviera en una misma jurisdicción; podría decirse incluso más: **seguiría siendo un problema asequible si se mantuviera en la jurisdicción nacional**.

3. Instituciones de cooperación policial internacional

Una de las primeras y más inmediata función de las organizaciones de cooperación policial internacional es la de actuar como canal de transmisión de las solicitudes de auxilio judicial internacional, cuando se opta por un canal policial por razones de urgencia, a saber: INTERPOL y EUROPOL.[21] Las razones de urgencia, si bien han de ser valoradas en última instancia por la autoridad judicial competente, tienen su origen en esta especialidad investigativa, en la gran volatilidad de los ficheros históricos de los proveedores de servicios. Sin embargo, en la mayoría de los casos, la información policial intercambiada entre agencias policiales de distintos países por canales oficiales puede recibir de las autoridades judiciales locales tanto valor como los informes de su propia policía. Las grandes operaciones internacionales se caracterizan porque concitan el interés directo de todos los países implicados, lo que trasciende al mero auxilio judicial.

3.1. La cooperación policial internacional actual en el ámbito de las investigaciones por Internet

La delincuencia en la Red ha evolucionado sobremanera desde las primeras operaciones internacionales. En materia de comunidades virtuales pedófilas, éstas son mucho más impenetrables, y sus miembros utilizan tecnología para la anonimización, la codificación y la eliminación de rastros que requieren otra estrategia de investigación, tal vez más a largo plazo. Las conexiones entre las redes de crimen organizado y los piratas informáticos configuran un tipo de delincuencia cuya respuesta policial es un continuo reto de actualización tecnológica.

17. Aclaremos que lo que tiene de adversativa esta proposición únicamente tiene que ver con la gestión y consumo de recursos por parte del investigador, requiriéndose, en muchas ocasiones, su personación ante la sede judicial.
18. Así lo previene el art. 282 de la Ley de Enjuiciamiento Criminal: «La Policía judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; **practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad Judicial**».
19. En ocasiones se han intentado otras medidas menos lesivas que la entrada y registro, con un resultado incierto; si bien la posibilidad de disponer de varias máquinas en el domicilio las hacen ya definitivamente ineficaces.
20. Podría llamar la atención que la tutela judicial en las fases tempranas de la investigación constituya un hecho excepcional; sin embargo, hasta que la comprobación del delito y el descubrimiento de los delincuentes adquiera un grado de maduración y concreción suficiente como para ser participado a la autoridad judicial, en otro tipo de delitos, pueden mediar multitud de gestiones de captación de inteligencia que pueden prolongarse mucho en el tiempo: *vigilancias, seguimientos, entrevistas...* Las investigaciones en Internet requieren un auto motivado por cada proveedor de servicios realmente implicado. Al final, también uno de entrada y registro.
21. El Convenio Europeo de asistencia judicial en materia penal (29 de mayo de 2000) establece en su artículo 6.4 que: «En caso de urgencia, las solicitudes de asistencia judicial podrán transmitirse por conducto de la Organización Internacional de Policía Criminal (INTERPOL) o de cualquier órgano competente según las disposiciones adoptadas en virtud del Tratado de la Unión Europea» (EUROPOL).

Con carácter general distinguimos tres vías de cooperación internacional policial:

a) Bilateral.[22] A través de los consejeros y agregados de Interior en las misiones diplomáticas permanentes del Reino de España. Este tipo de cooperación se caracteriza por:

- Utilización de las infraestructuras las misiones diplomáticas permanentes y personal orgánicamente adscrito a ellas.
- Comunicaciones personalizadas.
- Su operatividad merma con la aparición de terceros países.

b) Interpol. Sus principales finalidades son:

- Conseguir y desarrollar, dentro del marco de las leyes de los diferentes países y de la Declaración Universal de Derechos Humanos, la más amplia asistencia recíproca de las autoridades de policía criminal.
- Establecer y desarrollar todas las instituciones que puedan contribuir a la prevención y a la represión de las infracciones de derecho común.[23]

c) Europol. Cuyo objetivo se define como:

- Mejorar, en el marco de la cooperación entre los Estados Miembros de conformidad con el punto 9 del artículo K.1 del Tratado de la Unión Europea, la eficacia de los servicios competentes de los Estados Miembros y la cooperación entre los mismos con vistas a la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia internacional, en la medida en que existan indicios concretos de una estructura delictiva organizada y que dos o más Estados Miembros se vean afectados por las formas de delincuencia antes mencionadas, de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados Miembros.
- Para alcanzar los objetivos definidos, Europol desempeñará prioritariamente las siguientes funciones:
  - Facilitar el intercambio de información entre los Estados Miembros.
  - Recoger, compilar y analizar informaciones y datos.
  - Comunicar sin demora a los servicios competentes de los Estados Miembros los datos que les afecten y la relación entre los actos delictivos de los que hayan tenido conocimiento.
  - Facilitar las investigaciones en los Estados Miembros transmitiendo a las unidades nacionales toda la información pertinente al respecto.
  - Gestionar sistemas informatizados de recogida de datos que contengan los datos previstos en los artículos 8, 10 y 11 del Convenio Europol (Sistema de Información de Europol y ficheros de trabajo con fines de análisis).[24]

3.2. Ficheros analíticos: una cuestión de inteligencia

El almacenamiento y tratamiento informático de datos de carácter personal requiere del establecimiento de un marco legal adecuado en términos de protección de datos.

Las unidades policiales nacionales de inteligencia criminal se rigen por sus respectivas legislaciones nacionales, por cuyo cumplimiento velan las autoridades nacionales correspondientes; en España en concreto, la Agencia de Protección de Datos.

En el ámbito europeo, esta labor de inteligencia en el ámbito del crimen organizado y su propio mandato la lleva a cabo EUROPOL, y el organismo encargado del cumplimiento de la normativa sobre protección de datos de carácter personal es el llamado Europol Joint Supervisory Body.[25] Los «recipientes» en los que esos datos son tratados son los *AWF* (*analysis work file*) o ficheros con fines de análisis. Estos ficheros analíticos

22. Regulada por Real Decreto 1300/2006, de 10 de noviembre sobre Organización y Funciones de las Consejerías de Interior en las Misiones Diplomáticas de España.
23. Artículo 2 del Estatuto de la INTERPOL.
24. Artículos 2.1 y 3.1 del Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (**Convenio Europol**), hecho en Bruselas el 26 de julio de 1995.
25. http://europoljsb.consilium.europa.eu/.

son grandes bases de datos relacionales en los que se almacenan las contribuciones de inteligencia que realizan los Estados Miembros según un determinado criterio u orden de apertura. Los datos nuevos que se van incorporando son comparados con los ya existentes de todas las maneras posibles, incluyendo las técnicas de *data mining*.[26]

La aparición de *cruces* o *hits* da lugar a la elaboración de informes analíticos que incluyen hipótesis e *intelligence gaps* o *huecos de información,* sugiriéndose a la agencia policial que ha realizado la contribución o, en general, a todas las implicadas, que dirijan sus esfuerzos a resolver esas específicas incógnitas, materializándose de este modo casos concretos de la así llamada *intelligence-led policing*.[27]

Con esta poderosa herramienta puede decirse que el investigador ha conseguido trascender a dos principales limitaciones: aunar el mayor número de hechos semejantes que pudieran ser más o menos conexos, dando profundidad y perspectiva a los directamente investigados, y agotar todas la posibilidades de comparación entre ellos, más allá de los límites naturales de su retentiva e intuición. El fichero analítico de Europol es la respuesta policial natural a este tipo de criminalidad sin fronteras.

a) Fichero «Twins»

El fichero Twins tiene una especial preferencia por la comunidad pedófila que se expresa en inglés, aunque no excluye otras lenguas. Su propósito es apoyar a las autoridades competentes de los Estados Miembros, tal y como establece el Convenio de Europol, en la prevención y lucha contra las formas de criminalidad dentro del mandato de Europol asociadas con la actividad de redes criminales implicadas en la producción, venta o distribución de pornografía infantil y delitos asociados.

Caben aún un par de reflexiones sobre la propia pornografía infantil en el marco de las organizaciones policiales internacionales, que siquiera merecen mención.

- La primera tiene que ver con Interpol y con su base de datos de series de pornografía infantil, que contribuye de manera muy eficaz en la identificación de víctimas y agresores, dando continuidad en el mundo real a la virtualidad de los recursos gráficos distribuidos en la Red.

- La segunda se refiere de nuevo a Europol, que requiere de una definición más amplia que la que la circunscribe estrictamente al crimen organizado, en parte por esta especialidad delictiva de la distribución de pornografía infantil, cuya casuística en ocasiones no cumple con el requisito de delinquir con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material.[28] Parece que la competencia de Europol se va a dirigir más hacia la delincuencia grave transnacional que a las actuales organizaciones criminales.

b) Fichero «Terminal»

Su orden de apertura se dirige a los actos de *skimming* y *carding*.[29] Los múltiples datos que se deducen de intervenciones policiales en las que resultan detenidas personas portando tarjetas falsificadas, y el resultado de posteriores pesquisas constituyen paquetes de inteligencia idóneos para su inclusión en las bases de datos de Terminal. Los informes analíticos de este AWF están contribuyendo de manera determinante[30] a perfilar las redes de distribución de *dumps* y los flujos de capital en torno al *hacking*. Es decir, como ya se ha indicado, estas investigaciones policiales, que se refieren a hechos más o menos conectados en grandes espacios geográficos y temporales, no cuentan con una única fuente que pudiera haber burlado el trazado *ex post facto* a nivel de red, sino

26. Una actividad de extracción cuyo objetivo es descubrir hechos contenidos en las bases de datos.
27. http://www.fco.gov.uk/Files/kfile/Media%20brief%20-%20Intelligence-led%20policing%20annex.pdf.
28. Artículo 2.a de la Convención de las Naciones Unidas contra la delincuencia transnacional organizada, adoptada por la Asamblea General de las Naciones Unidas, el 15 de noviembre del 2000.
29. El *skimming* es el clonado ilícito de una tarjeta bancaria mediante la sustracción de la información contenida a través del copiado manual o electrónico de sus números (cuando se paga en comercios, restaurantes, etc.) o la instalación de dispositivos en cajeros automáticos que permiten realizar una copia de la banda magnética y la clave de acceso (generalmente mediante una cámara oculta). El *carding* se relaciona con el uso ilegítimo de tarjetas bancarias, principalmente en Internet.
30. http://www.europol.europa.eu/index.asp?page=news&news=pr070315.htm.

que en torno a estas transferencias de datos, que son clave, se circunscriben muchas otras, de muy variadas características técnicas y con una protección variable que pueden aportar inteligencia de gran valor analítico. El fichero Terminal procesaba a mediados del 2006 más de medio millón de entidades y más de 280.000 enlaces o relaciones; además, se beneficia especialmente de los acuerdos operativos suscritos por Europol con agencias policiales de EE. UU. y con Rusia, que permiten el intercambio de datos de carácter personal.

Conclusiones

La Red es una versión ampliada y mejorada del sistema nervioso de la Humanidad y sus nuevas posibilidades tienen que ver con su versatilidad y su interactividad. Esta nueva versión de las comunicaciones ha ampliado en la misma medida las posibilidades en cuanto a la comisión de actos criminales, tanto perfeccionando las herramientas y *modi operandi* para cometer los tipos delictivos bien conocidos, como haciendo surgir nuevos riesgos y amenazas: los que suponen la propia existencia de las máquinas que componen la Red.

La prevención y atenuación de esta faceta negativa de la Red, que puede afectar a la privacidad, seguridad, patrimonio e indemnidad sexual de sus usuarios y otras personas, requiere de contramedidas de concienciación, legislativas y de policía.

Las agencias de policía han evolucionado desarrollando unidades especiales cuyos miembros reciben formación permanente. Estas agencias de policía cooperan entre sí activamente, desarrollando herramientas conjuntas de inteligencia y análisis.

Así, a un fenómeno criminal que ignora las fronteras le ha de corresponder un tratamiento global, igualmente transparente al principio de territorialidad. Los *analysis work files* de Europol son el producto más elaborado para la coordinación de las investigaciones de esta comunidad policial internacional, y el que se está revelando como más eficiente contra este tipo de criminalidad.

Cita recomendada

LÓPEZ, Antonio (2007). «La investigación policial en Internet: estructuras de cooperación internacional». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

http://www.uoc.edu/idp/5/dt/esp/lopez.pdf

ISSN 1699-8154

Sobre el autor

Antonio López

Inspector del Cuerpo Nacional de Policía. Oficial de enlace en Europol. Spanish Desk

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

Primeras jornadas profesionales sobre la protección de datos en la Universidad

Maite Casado Cadarso

Fecha de presentación: julio de 2007
Fecha de aceptación: julio de 2007
Fecha de publicación: septiembre de 2007

Resumen
En el marco del III Congreso IDP, Internet, Derecho y Política, tuvo lugar la celebración de la 1.ª jornada profesional que analizó el tratamiento de datos en las universidades. Se puso de relieve la necesidad de tener una política clara de tratamiento de datos y de las correspondientes auditorías con el fin de garantizar el cumplimiento de la legislación. Estas medidas comportan a la larga un beneficio para la propia Universidad ya que suponen proteger la información –uno de los activos fundamentales– y contribuyen a la racionalización de los procesos y de los medios de que dispone la Universidad.

Palabras clave
protección de datos, auditorías, información, política de seguridad

Tema
Protección de datos

1st Professional Seminar on Data Protection at Universities

Abstract
Within the framework of the III ILP Conference on Internet, Law and Politics, the 1st Professional Seminar was held in order to analyse data processing at universities. The seminar emphasised the need for a clear policy on data processing, as well as the corresponding audits to ensure compliance with the existing legislation. Such measures will eventually prove beneficial to the University itself as they are intended to protect information – a fundamental asset – and help to rationalise the processes and resources that the University has at its disposal.

Keywords
data protection, audits, information, security policy

Topic
Data protection

Dentro del III Congreso Internet, Derecho y Política, tuvo lugar, el día 8 de mayo, la celebración de las primeras jornadas profesionales dedicadas a la protección de datos en la Universidad.

Estas jornadas contaron con la asistencia de profesionales y técnicos responsables de la protección de datos en las diferentes universidades catalanas, y tenían como objeto poder reflexionar y debatir sobre los diferentes problemas con los que se encuentra este colectivo en el desarrollo de sus tareas habituales.

Con el fin de poder abordar este tema desde una perspectiva práctica y de diálogo, que permitiera encontrar a los diferentes operadores posibles soluciones a los problemas que les comporta la aplicación de la normativa de protección de datos en el entorno universitario, se inició la jornada de trabajo con las exposiciones de dos especialistas en la materia: Ricard Martínez, profesor de Derecho constitucional de la Universitat Oberta de Catalunya, y Eugenio Fernández, director de Informática de la Universidad Rey Juan Carlos.

Los dos ponentes abordaron el tema desde la perspectiva de la propia experiencia, dado que ambos trabajan en universidades premiadas con el Premio a las Mejores Prácticas de las Administraciones Públicas Europeas en materia de protección de datos, que anualmente otorga la Agencia de Protección de Datos de la Comunidad Autónoma de Madrid.

El profesor Ricard Martínez planteó su ponencia sobre un argumento central: que la implantación de una política de protección de datos en la compleja realidad jurídica y técnica que presentan actualmente las universidades no es un hito inalcanzable con costes excesivos, sino un reto que comporta beneficios para el funcionamiento de la Universidad, porque, por una parte, supone proteger la información, que es uno de sus activos fundamentales y, por otra parte, contribuye a la racionalización de los procesos y de los medios de que dispone la Universidad.

Asimismo, manifestó que para conseguir este objetivo eran fundamentales determinadas herramientas, como la realización de auditorías en materia de protección de datos por parte de personal adscrito a la organización de la propia Universidad, el compromiso y apoyo necesarios por parte de los responsables de la estructura universitaria y el conocimiento de la necesidad de proteger los datos personales por parte de los usuarios de los diferentes sistemas de información de que dispone la Universidad.

Una vez alcanzado un primer nivel de protección de la información, el profesor Ricard Martínez manifestó su preferencia por un sistema basado en preauditorías en materia de protección de datos, es decir, un sistema preventivo del riesgo que detecte las necesidades que, en materia de protección de datos, pueda ir teniendo la respectiva Universidad.

Por su parte, Eugenio Fernández insistió en la necesidad de introducir la protección de datos dentro de un plan estratégico que comprometa en esta materia a cada universidad y que este plan estratégico se sitúe dentro de un plan integral con objetivos prefijados y acciones determinadas para realizar.

Este ponente manifestó que consideraba indispensable que existiera un compromiso por parte de los usuarios de los sistemas de información y concluyó que, a su entender, era fundamental que el responsable de los ficheros o tratamientos no fuera la Universidad o un alto responsable dentro de su estructura organizativa, sino que consideraba más eficaz que se designaran como responsables de los tratamientos los órganos concretos que, en la práctica, gestionan y deciden respecto de cada aplicativo informático o tratamiento de datos.

Eugenio Fernández señaló también que es necesario disponer de especialistas informáticos que conozcan de manera detalla este ámbito material, así como la importancia de que el personal que trabaja en las universidades tenga también conocimientos en materia de protección de datos, dado que los usuarios de la información tienen que ser conscientes de la importancia del activo con el que trabajan, tanto a efectos de poder determinar las necesidades en materia de protección de datos como para contribuir a la implementación de las medidas de seguridad necesarias.

Las dos ponencias, dado su planteamiento práctico y ameno, generaron un debate dinámico donde los asistentes pudieron plantear diferentes cuestiones y problemas que los ponentes analizaron proponiendo posibles soluciones concretas. El debate fue moderado por Maite Casado, jefe del Área de Inspección de la Agencia Catalana de Protección de Datos, que pudo aprovechar la

ocasión para recordar a los asistentes las competencias de esta agencia en relación con las universidades ubicadas en el territorio de Cataluña, así como las cuestiones que, en relación con la materia de protección de datos en el ámbito universitario, han llegado hasta las diferentes autoridades de control que velan por el derecho fundamental a la autodeterminación informativa.

Cita recomendada

CASADO, Maite (2007). «Primeras jornadas profesionales sobre la protección de datos en la Universidad». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

<http://www.uoc.edu/idp/5/dt/esp/casado.pdf>

ISSN 1699-8154

Sobre la autora

Maite Casado

Licenciada en Derecho por la UAB. Máster en Derecho penal por la UB. Funcionaria facultativa licenciada en Derecho del Cuerpo de Mossos d'Esquadra. Abogada habilitada por el Gabinete Jurídico de la Generalitat. Jefe del Área de Inspección de la Agencia Catalana de Protección de Datos.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad*

Elisenda Bru Cuadrada

Fecha de presentación: abril de 2007
Fecha de aceptación: junio de 2007
Fecha de publicación: septiembre 2007

Resumen

El imparable avance de las tecnologías de la información y la comunicación en la sociedad actual facilita el tratamiento e intercambio de datos en los diferentes sectores de actividad económica y social. Este tratamiento masivo que las TIC posibilitan, puede acarrear riesgos para la intimidad, lo que hace necesario dotar de protección específica a este ámbito de los derechos del individuo. En el ámbito europeo, la Directiva 95/46/CE se aprueba con la voluntad de acercar las legislaciones estatales de protección de datos personales de los Estados Miembros de la Unión. La transposición de esta directiva en los distintos Estados debe establecer, entre otros aspectos, el régimen de infracciones y sanciones que habrá que aplicar en caso de incumplimiento de las disposiciones adoptadas en la materia. Por otra parte, la legislación penal protege también ciertos ámbitos del derecho a la intimidad en los ordenamientos jurídicos de los diferentes Estados. El presente trabajo analiza las similitudes y diferencias en los mecanismos jurídicos de protección del derecho a la intimidad en España, Alemania, Francia, Italia y Suecia a través del estudio del régimen sancionador previsto en sus legislaciones. La conclusión a la que se llega es que las diferencias entre ordenamientos existen, a pesar del espíritu de la directiva, que perseguía como objetivo esencial la armonización en el nivel de protección de datos personales en todos los Estados Miembros.

* El contenido de este artículo coincide, en lo fundamental, con la comunicación presentada en el *III Congreso Internet, Derecho y Política* (*IDP*). *Nuevas perspectivas*, organizado por los Estudios de Derecho y Ciencias Políticas de la UOC. La comunicación, que se ubica en la actividad del Grupo de Investigación DEUSETIC (Derecho Europeo de la Seguridad y TIC), obtuvo el primer premio *ex aequo* junto a la presentada por Isabel García Noguera.

Palabras clave
intimidad, protección de datos, autodeterminación informativa, *habeas data*

Tema
Protección de datos

Data protection in Spain and the European Union. Special reference to the legal mechanisms for reacting against breaches of our right to privacy.

Abstract
The unstoppable advance of information and communication technologies in today's society facilitates the processing and exchange of data within the different sectors of economic and social activity. Such en masse processing enabled by ICTs may jeopardise our privacy, making it necessary to establish specific protection for this area of individual rights. In the European ambit, Directive 95/46/CE was created in order to approximate the state legislation on personal data protection that exists in the EU member states. The transposition of the Directive in the different States must establish, among other aspects, the infraction and sanction system to be applied in the event of non-compliance with the regulations adopted in this matter. Furthermore, penal legislation also protects certain areas of our right to privacy in the legal regulations that exist in the different member States. This work analyses the similarities and differences within the legal mechanisms for protecting our right to privacy in Spain, Germany, France, Italy and Sweden by studying the sanctioning system envisaged in their legislations. The conclusion reached is that differences indeed exist between the regulations, despite the spirit of the Directive, whose main objective was to harmonise the level of personal data protection in all member States.

Keywords
privacy, data protection, informative self-determination, habeas data

Topic
Data protection

Introducción

Las tecnologías de la información y la comunicación multiplican la velocidad de tratamiento de la información, la capacidad de almacenamiento y la de transmisión de los datos. Existe un enorme flujo de información, que circula constantemente sin que los afectados sean conscientes de ello. Esta situación es susceptible de vulnerar algunos de los derechos básicos de la persona, que puede ver reducido su ámbito de privacidad por el tratamiento intenso y global de sus datos personales. La necesidad de otorgar protección específica frente a las nuevas amenazas derivadas de este contexto ha conducido al desarrollo de normas *ad hoc* en la mayoría de los sistemas jurídicos de nuestro entorno.[1]

El tratamiento automatizado de datos de carácter personal en los últimos tiempos ha sido objeto de especial atención por parte del derecho internacional, comunitario e interno de los Estados Miembros de la Unión Europea. En paralelo al desarrollo de la llamada sociedad de la información, se ha suscitado un amplio debate sobre las políticas existentes en materia de protección de datos y sobre las estrategias más adecuadas para la salvaguarda de este derecho.

El objeto de esta comunicación es ofrecer una visión general del estado actual de la legislación en materia de protección del derecho a la intimidad, especialmente en lo relativo a protección de datos de carácter personal. Nos centraremos en el análisis del régimen sancionador previsto en las diferentes leyes administrativas y penales. Se pretende comparar las infracciones y sanciones en distintos Estados Miembros de la UE. En concreto, se ha decidido centrar el estudio en los ordenamientos jurídicos de España, Alemania, Francia, Italia y Suecia.

1. El derecho fundamental a la intimidad

El reconocimiento del derecho a la intimidad sirvió a la sociedad burguesa para protegerse frente al intervencionismo y arbitrariedad de los poderes públicos. La intimidad suponía una faceta de autonomía, aislamiento y exclusión frente a las intervenciones públicas en la vida privada. La concepción liberal equiparó la intimidad a un objeto más entre las posesiones privadas del individuo. Posteriormente, nuevas necesidades de protección fueron surgiendo y la concepción patrimonial del derecho sufrió cambios importantes.

Es comúnmente aceptado que el concepto jurídico de intimidad tuvo su origen en un artículo de los juristas WARREN y BRANDEIS,[2] en el que se reclamó la necesidad de reconocimiento de un nuevo derecho, el derecho a la intimidad, necesario para proteger a la persona frente a las intromisiones de los medios de comunicación. Se buscaba un límite jurídico que vedase las intromisiones de la prensa en la vida privada, para evitar las lesiones que la difusión generalizada de hechos relativos a la vida privada podía provocar. Con todo, el derecho a la intimidad debía a su vez limitarse para convivir con otros bienes y derechos fundamentales, como la libertad de expresión y el derecho a la información.

A partir del momento de este reconocimiento, el derecho a la intimidad pierde su vertiente más patrimonial para consagrarse como el derecho que posee toda persona para protegerse de las intrusiones ajenas. Con ello, la libertad individual pasa a ser el fundamento del derecho a la intimidad, que deja de ser un derecho de propiedad.

El reconocimiento constitucional del derecho vendrá posteriormente, si bien las distintas constituciones lo recogerán de forma diversa. Así, pueden distinguirse ordenamientos en que la intimidad tiene un reconocimiento pleno a nivel constitucional (Bélgica, Países Bajos, España),[3] otros que recogen simplemente manifestaciones del derecho (Alemania, Italia, Dinamarca)[4] y por último, ordenamientos que no recogen en sus constituciones ni el derecho ni sus manifestaciones (Francia),[5] pero tienen un reconocimiento legal.

La doctrina[6] suele asignar al derecho a la intimidad las siguientes características. En primer lugar, se trata de un derecho de la personalidad, subjetivo y de defensa.

1. El avance tecnológico conduce a dos fenómenos profundamente interrelacionados. De un lado, el fenómeno de la contaminación de las libertades, es decir, la erosión de los derechos fundamentales por influjo de las nuevas tecnologías. De otro lado, la reivindicación y el alumbramiento de una nueva generación de derechos fundamentales que conduce a una nueva interpretación de los derechos tradicionales. *Víd*., en este sentido, R. MARTÍNEZ MARTÍNEZ (2001). *Tecnologías de la información, policía y Constitución*. Valencia: Tirant Lo Blanch. Pág. 48-49. Y el mismo autor (2004). *Una aproximación crítica a la autodeterminación informativa* . Madrid: Thomson-Civitas. Págs. 45 y sig.
2. S. D. WARREN; L. D. BRANDEIS (1890). «The right to privacy». *Harvard Law Review*. Vol. IV, n.º 5, pág. 193-219. Traducción al castellano de BENIGNO PENDÁS y PILAR BASELGA (1995). *Derecho a la intimidad*. Madrid: Civitas. *Vid*., un estudio en profundidad sobre la evolución del derecho a la intimidad y, en especial, del significado de la obra de WARREN y BRANDEIS en la protección de la intimidad, en R. MARTÍNEZ MARTÍNEZ. *Una aproximación crítica a la autodeterminación informativa*. *Op. cit*. Pág. 61 y sig.
3. Constitución belga de 1994 (art. 22), Constitución holandesa de 1983 (art. 10) y Constitución española de 1978 (art. 18).
4. Constitución alemana de 1949 (arts. 1, 2, 10.1, 13), Constitución italiana de 1947 (arts. 14 y 15) y Constitución danesa de 1953 (art. 72).
5. Constitución francesa de 1946.
6. L. REBOLLO DELGADO (2005). *El derecho fundamental a la intimidad*. Madrid: Dykinson. Pág.117-125. P. LUCAS MURILLO DE LA CUEVA (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos. Pág. 77-88. M. CARRILLO LÓPEZ (2003). *El derecho a no ser molestado*. Navarra: Aranzadi. Pág. 30-31.

No es sólo la potestad que tenemos de que un tercero conozca o no nuestra vida privada, sino también la posibilidad de controlar lo que otros conocen de nosotros. Es derecho positivo, inserto en la Constitución y configurado como un derecho de rango superior y, por tanto, protegido por las garantías cualificadas previstas en su artículo 53. Se configura como garantía de libertad. La libertad se erige en elemento necesario de la dignidad humana y los derechos de la personalidad en elementos integradores del concepto de libertad. Es, por último, un derecho irrenunciable, imprescriptible, inalienable, intransmisible e inembargable.

Debido a la aparición de nuevos ámbitos de protección, a partir del desarrollo de las tecnologías de la información y la comunicación, la doctrina ha abierto un amplio debate sobre la distinción entre intimidad[7] y privacidad.[8] El debate se acentúa con la aparición de nuevos conceptos jurídicos como la llamada «autodeterminación informativa», «libertad informática», «intimidad informática» o «derecho a la protección de datos personales». Tanto la doctrina como la jurisprudencia han estudiado el origen y la naturaleza jurídica de este derecho. Hay opiniones a favor de la consideración del mismo como derecho fundamental autónomo,[9] mientras no faltan quienes argumentan que se trata de una reformulación del derecho a la intimidad.[10]

2. La intimidad informática: el derecho a la autodeterminación informativa o derecho a la protección de datos personales

El derecho a la autodeterminación informativa surge como respuesta a la posibilidad de un tratamiento masivo de datos. Fue construido y elaborado a partir de la sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983.[11] En dicha sentencia, el Tribunal configura, a partir del derecho general de la personalidad recogido en el artículo 2.1 de la Ley Fundamental de Bonn, la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo, cuándo y dentro de qué límites, procede revelar situaciones referentes a la vida propia. Surge la necesidad de establecer jurídicamente mecanismos de protección de los datos personales frente a su uso informatizado, no tanto por el carácter estrictamente privado de éstos, sino por el peligro que supone la utilización que se haga de los mismos.

En todo caso, el derecho no comporta una patrimonialización de los datos personales, sino que es la garantía de una serie de facultades individuales que permitirán al titular llevar a cabo el control y seguimiento de la información personal registrada en soportes informáticos.

En cuanto a la naturaleza jurídica del derecho, no se discute que se trata de un derecho de la personalidad, que se caracteriza por ser connatural e innato, subjetivo y privado, oponible *erga omnes,* inherente a la persona, necesario para el pleno desarrollo de la personalidad, intransmisible, irrenunciable, inembargable, indisponible e imprescriptible.[12]

En palabras del TC español, «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionará a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o no».[13]

7. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.
8. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.
9. L. M. DÍEZ-PICAZO GIMÉNEZ (2003). *Sistema de Derechos Fundamentales*. Madrid: Civitas. Pág. 277. P. LUCAS MURILLO DE LA CUEVA. *Op. cit*. Pág.147-196; R. MARTÍNEZ MARTÍNEZ. *Una aproximación crítica a la autodeterminación informativa. Op. cit*. Pág. 34; STC 144/1999 y 292/2000.
10. L. REBOLLO DELGADO. *Op. cit*. Pág. 135. Más ampliamente, sobre este debate, M. I. HERRÁN ORTIZ (2002). *El derecho a la intimidad en la nueva Ley Orgánica de protección de datos personales*. Madrid: Dykinson. Pág.77-87.
11. BJC1984, n.º 33, pág. 126-170.
12. Para una profundización sobre las características de este derecho, véanse, P. LUCAS MURILLO DE LA CUEVA. *El derecho a la autodeterminación informativa* (...). *Op. cit*.; R. MARTÍNEZ MARTÍNEZ. *Una aproximación crítica* (...). *Op. cit.* Pág. 33 y sig.
13. STC 292/2000, de 30 de noviembre, FJ 6 y 7.

3. Las iniciativas de la Unión Europea en materia de protección de datos: el Convenio 108 del Consejo y la Directiva 95/46/CE

En 1981 se aprobó el Convenio n.º 108 del Consejo, sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, primera norma europea que marcó las pautas del modelo común de protección de datos. El Convenio pretendía ampliar la protección de los derechos y las libertades fundamentales y, en concreto, el derecho al respeto a la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos informatizados.[14]

El objeto del Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sea cual sea su nacionalidad o 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 (art. 1).

El convenio[15] recoge en su capítulo segundo unos principios básicos para la protección de datos: principio de lealtad, principio de exactitud, principio finalista, principio de pertinencia, principio de utilización no abusiva, principio del derecho al olvido, principio de publicidad, principio de acceso individual, principio de seguridad, principio de prohibición de tratamiento automático de datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas o de otro tipo, o datos relativos a la salud o vida sexual, a menos que el derecho interno prevea garantías adecuadas.[16]

En cuanto al régimen sancionador previsto en el convenio, el artículo 10 remite la adopción del mismo a los Estados Parte. El convenio deja completamente abierta la cuestión relativa no sólo al tipo de sanciones que pueden preverse, sino también al sector jurídico en el que pueden integrarse.

Sobre la base de los principios aportados por el Convenio mencionado, fue aprobada en el ámbito comunitario la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. La Directiva sienta las bases para lograr la coordinación de las legislaciones nacionales aplicables en materia de protección de datos en aras a garantizar la libre circulación de tales datos entre los Estados Miembros.[17] Los principios de protección de los derechos y libertades de las personas, y concretamente, del respeto a la intimidad, que se contienen en la directiva, vienen a ampliar los del convenio, y así se desprende del Considerando 11 de la misma.

La directiva establece los principios y requisitos procedimentales que deberán considerarse exigencia mínima para que la protección sea adecuada. Hablamos de dos tipos de principios: los que se tendrán en cuenta en el momento de recoger los datos y los que se tendrán en cuenta durante el tratamiento o procesamiento de los datos.

En el momento de recabar los datos, siguiendo las disposiciones del artículo 6, estos deberán ser tratados de manera leal y lícita (principio de lealtad); recogidos con fines determinados, explícitos y legítimos y no tratados posteriormente de manera incompatible con dichos fines (principio de finalidad y principio de utilización no abusiva); adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de pertinencia); exactos y, cuando sea necesario, actualizados (principio de exactitud); conservados durante un tiempo no superior al necesario para los fines para los que fueron recogidos (principio del derecho al olvido). El artículo 8 establece el principio de prohibición de tratamiento de datos personales relativos al origen racial o étnico, a las convicciones religiosas o filosó-

14. Puede consultarse el estado de adhesiones al convenio en el siguiente enlace: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG
15. Disponible en: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
16. La clasificación es de P. LUCAS MURILLO DE LA CUEVA. *Op. cit*. Pág. 142-143. *Vid*., también, ampliamente, R. MARTÍNEZ MARTÍNEZ. *Una aproximación crítica* (...). *Op. cit*. Pág. 155 y sig.
17. *Vid*. Considerando n.º 7 de la directiva.

ficas, la pertenencia a sindicatos y los datos relativos a la salud y sexualidad. En su apartado segundo determina los casos en que el citado principio no será de aplicación. Finalmente, de acuerdo con lo establecido en los artículos 10 y 11, deberá regir el principio de información.

En el momento del tratamiento o procesamiento de los datos, habrá que tener en cuenta los principios de confidencialidad de los datos recogidos (art. 16), seguridad (art. 17) y consentimiento del interesado (art. 7). Por último, el interesado gozará del principio de acceso individual, mediante los derechos de acceso y oposición (arts. 12 y 14).

El capítulo III de la directiva lleva por título «Recursos judiciales, responsabilidad y sanciones». De la misma forma que lo hiciera el convenio, la directiva remite a los Estados el establecimiento de los recursos y las sanciones necesarias para los supuestos de infracción de la normativa.

Con el artículo 22 el legislador comunitario da la opción de que se prevea un recurso de naturaleza administrativa ante las autoridades de control sujetas al derecho administrativo. Este recurso es opcional, pero no lo es el recurso judicial, que deberá existir en todas las legislaciones nacionales.

Por lo que respecta al régimen de responsabilidad, el artículo 23 establece que los Estados Miembros dispondrán que toda persona que se vea perjudicada como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la directiva tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho causante del daño. En este sentido, el Considerando 55 de la directiva añade que el daño habrá de ser reparado por el responsable del tratamiento a no ser que éste pruebe que no le es imputable, principalmente si demuestra la responsabilidad del interesado o que se trata de un caso de fuerza mayor.

En cuanto a las sanciones, el artículo 24 determina que los Estados Miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la directiva y determinarán las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la misma.

El Considerando 55 precisa que las sanciones se impondrán a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente directiva.

4. La legislación sobre protección de datos en algunos Estados Miembros de la UE

A continuación se estudian las leyes de protección de datos de España, Alemania, Francia, Italia y Suecia. Este trabajo se centra en los ordenamientos jurídicos de los citados Estados, por varios motivos. En algún caso, por ser pioneros en la promulgación de normas protectoras del derecho a la protección de datos de carácter personal; en otros porque lo fueron respecto de la implementación de la directiva; o, finalmente, por razones de proximidad jurídica con el sistema español, lo que facilita la posibilidad de realizar un estudio comparativo.

4.1. La legislación española

En España el derecho a la intimidad viene recogido en el artículo 18 de la Constitución, que acoge un contenido amplio de intimidad. Junto a la declaración general de positivización del derecho, se reconocen específicamente algunas facetas del mismo como la intimidad domiciliaria, la libertad y confidencialidad de las comunicaciones privadas o el secreto de las comunicaciones, para acabar con la constitucionalización del *habeas data* o faceta informática de la intimidad.[18]

El derecho a la intimidad se recoge en la sección primera del capítulo II del título I de la CE, donde se proclaman los derechos fundamentales. Ello conlleva que goce de las máximas garantías que el ordenamiento jurídico establece para dichos derechos.

18. Así lo reconoce el TC en la STC 254/1993, F. J.6.

El desarrollo legislativo del derecho se lleva a cabo mediante dos leyes: la Ley Orgánica 1/82, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen y la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal[19] (en adelante, LOPD).

La finalidad de la LO 1/82 es establecer, dentro del ámbito del derecho civil, los límites en virtud de los cuales puede constatarse que tiene lugar una lesión al derecho. La lesión se verificará cuando se produzca una intromisión ilegítima, siempre que ésta no sea constitutiva de delito, puesto que en este caso se estaría a lo dispuesto en el Código penal, aplicándose, eso sí, lo previsto en la LO 1/82 para la determinación de la responsabilidad civil derivada del delito (art. 2). El artículo 7 de la ley define los casos de intromisión ilegítima. Frente a tales intromisiones, la ley prevé medidas de protección: acción declarativa, acción de cesación y abstención, acción de reparación e indemnización por daños y perjuicios (que se extenderá al daño moral, valorable según las circunstancias del caso y la gravedad de la lesión producida). Las acciones de protección caducarán transcurridos cuatro años desde que el legitimado pudo ejercitarlas (art. 9).

La LOPD supuso la derogación de la Ley Orgánica 5/92, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (en adelante, LORTAD) y la transposición de la Directiva 95/46/CE a nuestro ordenamiento interno. El objeto de la LOPD es garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, en lo que concierne al tratamiento de datos personales (art. 1).

El título VII de la LOPD determina el régimen sancionador. La LOPD no incluye conductas delictivas, por considerarse que de ser así se estarían creando delitos de segunda categoría, de difícil aplicación en la práctica.

Las infracciones se califican como leves, graves y muy graves (art. 44). El artículo 45 cataloga los distintos tipos de sanciones imponibles, clasificadas en función de la gravedad. Las infracciones leves serán sancionadas con multa de 601,01 euros a 60.101,21 euros, las infracciones graves se castigarán con multa de 60.101,21 euros a 300.506,05 euros y las infracciones muy graves con multa de 300.506,05 euros a 601.012,10 euros. La cuantía de las sanciones 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, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora (art. 45.4 LOPD). Por último, merece atención el párrafo 5.º del artículo 45, que permite al órgano sancionador, el director de la Agencia Española de Protección de Datos (AEPD), rebajar la cuantía de la sanción, aplicando la escala precedente a la que corresponda a la tipicidad de los hechos sancionados, en caso de apreciar una cualificada disminución de la culpabilidad o de la antijuricidad. Así, aun manteniéndose la infracción como grave, el infractor puede ser sancionado con una multa correspondiente a la infracción leve en cualquiera de sus tres grados. Se trata de un supuesto excepcional que deberá ser motivado y cuya resolución podrá ser revisada por la jurisdicción contencioso-administrativa.

El artículo 43 establece el régimen de responsabilidad y en su apartado primero determina que los responsables de los ficheros[20] y los encargados de los tratamientos[21] estarán sujetos al régimen sancionador establecido en la presente ley. Se desprende de este precepto que las sanciones administrativas se impondrán tan sólo en el caso de que se produzca una conducta ilícita por parte de quien es responsable del fichero o encargado del tratamiento. Por ello, las conductas que se tipifican como infracción hacen referencia a trámites u obligaciones previstas en la ley para este tipo de sujetos.

19. Actualmente, existe un proyecto de reglamento de desarrollo de la ley, que se encuentra en fase avanzada de aprobación y que derogaría al RD 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación de los Datos de Carácter Personal, y el RD 994/1999, de 11 de junio.
20. Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
21. Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo, o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Finalmente, el artículo 46 de la ley prevé el caso en que las infracciones se cometan en ficheros de los que sean responsables las administraciones públicas. En dicho supuesto, el director de la AEPD resolverá sobre las medidas correctoras a aplicar y podrá proponer también la iniciación de actuaciones disciplinarias. El procedimiento y las sanciones aplicables serán los establecidos en la legislación sobre régimen disciplinario de las administraciones públicas.

En cuanto a las sanciones penales, éstas se recogen en el título X del Código penal (CP). El ordenamiento penal recoge, salvo algunas excepciones, un sistema abierto de posibles sujetos pasivos, por lo que permitirá, en principio, el castigo de todo aquel que realice la conducta típica. En el tipo básico del art. 197 CP se definen, de un modo especialmente casuístico, las distintas modalidades delictivas. Tras tipificar las diferentes conductas lesivas de la intimidad con relevancia penal, el apartado segundo se dedica íntegramente a la protección de la autodeterminación informativa, incriminando los abusos perpetrados sobre datos personales registrados en ficheros automatizados o en cualquier otro tipo de archivo o registro público o privado. Se prevé, además, un tipo agravado para los casos de difusión, revelación o cesión a terceros de los datos (art. 197.3 CP). La condición profesional del sujeto activo del delito (el responsable del fichero o encargado del tratamiento), se toma en consideración para la creación de un subtipo agravado en el apartado cuarto, que permite imponer una pena de entre tres y cinco años de prisión, salvo que, además, los datos se difundan, cedan o revelen, en cuya caso la pena se elevará hasta su mitad superior. Si la conducta incurre en la afectación del núcleo duro del derecho, o la víctima es un menor o incapaz, se incurre en otro subtipo cualificado previsto en el apartado quinto. Por último, el apartado sexto prevé un tipo agravado para los casos en que la conducta delictiva se haya realizado con fines lucrativos. El artículo 197.3 CP apartado segundo, por su parte, prevé un tipo autónomo para los casos en que el autor, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, difunda, revele o ceda a terceros los datos. Finalmente, el artículo 198 CP prevé un tipo agravado para el caso de autoridades y funcionarios públicos que realizaren cualquiera de las conductas previstas en el artículo anterior. En este caso se aplicarán las penas previstas en su mitad superior y la pena de inhabilitación absoluta de seis a doce años.[22]

Las penas previstas oscilan, por tanto, entre la pena de prisión de uno a tres años, hasta la pena de prisión de cuatro a siete años, para el caso en que se realice la conducta con fines lucrativos y además afecte al núcleo duro del derecho.

Pese a la naturaleza subsidiaria y fragmentaria del Derecho penal su carácter, en definitiva, de *ultima* ratio, que condiciona su intervención únicamente cuando resulte necesaria, porque los instrumentos extrapenales no resulten adecuados para la correcta protección de los bienes jurídicos, y únicamente para los ataques más graves, no siempre resulta sencillo distinguir materialmente entre las infracciones contenidas en la LOPD y las previstas en el Código penal.

Sí es cierto que, conforme al ya citado artículo 43.1 LOPD, los destinatarios del régimen sancionador previsto en esta ley son únicamente los responsables de los ficheros y los encargados del tratamiento, por tanto son los únicos sujetos activos posibles de las infracciones allí recogidas. Al margen quedan, pues, los *outsiders*. Pero conviene recordar que restaría aún la protección dispensada por la LO 1/82, como ha puesto de relieve la doctrina, para aquellas intromisiones en el derecho no abarcadas por la LOPD y, en especial, para las llevadas a cabo por los *outsiders*, a pesar de que la concreción típica en el caso de la intromisión no esté depurada y actualizada.[23]

MORALES PRATS, consciente de este solapamiento, mantiene que si se intenta hallar algún criterio de selección entre las conductas incriminadas en el Código penal y las que han sido ubicadas en sede administrativa, se observará la imposibilidad de dar *con un*

22. *Vid., in extenso*, F. MORALES PRATS. *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*. En: VARIOS AUTORES. *Comentarios al Nuevo Código Penal*. G. QUINTERO OLIVARES (dir.) (2004). Navarra: Thomson-Aranzadi. 3.ª ed. pág. 1038 y sig.
23. E. ANARTE BORRALLO (2003). *Sobre los límites de la protección penal de datos personales*. En: *Derecho y conocimiento*. Universidad de Huelva, Vol. 2, pág. 225-254.

reparto de funciones entre infracción penal e infracción administrativa. Ante esta situación, los particulares pueden, en los términos establecidos en el artículo 201 del CP, dejar de lado la vía penal y optar por la civil o administrativa.[24]

4.2. La legislación alemana[25]

La Constitución alemana, de 23 de mayo de 1949, no prevé ningún precepto donde se reconozca directamente el derecho a la intimidad personal y familiar, tal y como se recoge en la Constitución española. No obstante, el párrafo 1 de la Constitución alemana establece la inviolabilidad de la dignidad humana y el párrafo 2 reconoce la garantía al libre desarrollo de la personalidad y la inviolabilidad de la persona. Por su parte, el párrafo 10.1 reconoce la privacidad de las cartas y el secreto de las comunicaciones y el párrafo 13 establece la inviolabilidad del domicilio. En cuanto a la protección de la intimidad informática, es importante recordar la sentencia del Tribunal Federal alemán de 15 de diciembre de 1983, en la que se recogen las bases y los elementos básicos del contenido del derecho a la protección de datos de carácter personal.[26]

En Alemania, la transposición de la Directiva 95/46/CE se llevó a cabo a mediante la Ley Federal de Protección de Datos, adoptada el 18 de mayo del 2001. La parte V de la ley recoge las disposiciones finales, dentro de las que encontramos los párrafos 43 y 44, que determinan las infracciones administrativas y penales, respectivamente.

El párrafo 43 incluye como infracciones sancionables administrativamente, aquellas realizadas por cualquiera que intencionadamente o por negligencia lleve a cabo alguna de las conductas previstas en el apartado primero o en el apartado segundo del precepto. A diferencia de la ley española, la ley alemana no especifica los sujetos destinatarios de la norma. Bastará con realizar la conducta típica para ser sancionado.

El apartado tercero del párrafo 43 prevé que las infracciones incluidas en el apartado primero serán castigadas con multa de 25.564 euros y las infracciones incluidas en el apartado segundo serán castigadas con multa de hasta 255.645 euros.

La norma alemana prevé infracciones penales y sus consecuencias dentro de la misma ley de protección de datos. El párrafo 44 establece estas infracciones. El apartado primero prevé como infracción sancionable con hasta dos años de cárcel o multa cometer deliberadamente un acto de los previstos en el apartado segundo del párrafo 43 con la intención de enriquecerse uno mismo o a otro o con intención de perjudicar a un tercero. El apartado segundo especifica que estos delitos sólo serán perseguibles mediante denuncia del titular de los datos o de la autoridad de control.

Por su parte, el Código penal alemán dedica su capítulo 15 a la violación de la esfera de la privacidad personal y la confidencialidad y, dentro de éste, su párrafo 202a lleva por título «Espionaje de datos». Este precepto se compone de dos apartados. El primero de ellos establece que cualquier persona que obtenga datos personales sin autorización, para sí o para un tercero, especialmente protegidos contra el acceso no autorizado, podrá ser castigado con una pena de prisión no superior a tres años o una multa. Datos personales, según el apartado segundo de este párrafo, lo serán sólo aquéllos guardados o transmitidos electrónica o magnéticamente, o de un modo no percibible de forma inmediata. El legislador alemán, a diferencia del español, no define el abanico de conductas punibles y tampoco prevé tipos agravados o hiperagravados.

4.3. La legislación francesa

La Constitución francesa de 1958[27] forma parte de aquellos ordenamientos que no recogen el derecho a la intimidad de forma concreta y que tampoco establecen con rango constitucional la garantía de manifestaciones clásicas del derecho. Sin embargo, ello no implica ausencia

24. F. MORALES PRATS. *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*. *Op. cit*. Pág. 1047.
25. Puede consultarse una versión traducida al castellano del texto de las diferentes constituciones de los Estados Miembros de la Unión Europea, en la página web: http://www.constitucion.es/otras_constituciones/europa/index.html
26. *Vid*., más detalladamente sobre la legislación alemana y el alcance de la resolución citada, R. MARTÍNEZ MARTÍNEZ. *Una aproximación crítica*. *Op. cit*. Pág. 237 y sig.

del reconocimiento del derecho, dado que puede tener su engarce en otras disposiciones de la norma fundamental[28] y posee, de hecho, cobertura legal.

El reconocimiento legal lo proporciona la Ley n.º 2004-801 de 6 de agosto del 2004, relativa a la protección de las personas físicas respecto al tratamiento de datos de carácter personal, norma que supone la transposición de la directiva al ordenamiento jurídico francés. El capítulo VII lleva por título «Sanciones pronunciadas por la Comisión Nacional de la informática y las libertades» y recoge las sanciones administrativas. El capítulo VIII hace referencia a las disposiciones penales.

El artículo 45 de la ley establece los casos en que la Comisión Nacional de la Informática y las Libertades podrá intervenir cuando se haya producido una infracción. Los mecanismos que la comisión posee para disuadir a los infractores son diversos. Así, la comisión puede advertir al infractor, imponerle una multa, conminarlo para detener el tratamiento o retirarle la autorización, interrumpir o cerrar automáticamente el tratamiento durante 3 meses, informar al primer ministro o presentar un recurso de urgencia ante la jurisdicción competente para que adopte las medidas necesarias para la salvaguardia de derechos y libertades.

Las sanciones previstas en el artículo 45.I y 45.II.1.º serán pronunciadas por medio de un informe establecido por uno de los miembros de la comisión, designado por el presidente de ésta, de acuerdo con el artículo 46 de la ley. El informe se notificará al responsable del tratamiento, quien podrá prestar declaración y hacerse representar o asistir.

El artículo 47 de la ley prevé las multas aplicables, que serán proporcionales a la gravedad de las infracciones cometidas y a los beneficios obtenidos de la infracción. La primera infracción no se podrá castigar con una multa superior a 150.000 euros. En caso de infracción reiterada dentro de los cinco años a contar desde la fecha de aquélla sanción pecuniaria precedentemente pronunciada y convertida en definitiva, la multa no podrá superar los 300.000 euros.

El capítulo VIII incluye las sanciones penales. El artículo 50 hace una remisión a los artículos 226-16 a 226-24 del Código penal. El artículo 51 castiga con un año de prisión y multa de 15.000 euros el hecho de obstaculizar la acción de la Comisión Nacional de la Informática y de las Libertades.

En cuanto a los delitos, éstos se comprenden en el capítulo VI del Código penal, que trata los delitos contra la personalidad, concretamente en su sección quinta, que lleva por nombre «Los atentados contra los derechos de las personas resultantes de los ficheros o de los tratamientos informáticos» y comprende los artículos 226-16 a 226-24.

El legislador francés prevé la misma pena para todos los tipos delictivos (cinco años de prisión y multa de 300.000 euros), a excepción de los casos de divulgación imprudente o negligente, en los que la pena será de tres años de prisión y multa de 100.000 euros.

4.4. La legislación italiana

La Constitución italiana de 27 de diciembre de 1947 no realiza mención expresa de la intimidad como derecho, pero recoge manifestaciones de la misma, reconociendo de forma correlativa la inviolabilidad del domicilio (art. 14) y el secreto de las comunicaciones (art. 15).

La Directiva 95/46/CE se transpone mediante el *Codice in materia di protezione dei dati personali,* de 30 de junio del 2003. La parte III del código lleva por título «Tutela del interesado y sanciones». El título III regula las sanciones, que se dividen en dos capítulos. El capítulo I establece

27. Téngase en cuenta que el contenido de la vigente Constitución francesa de 1958 debe integrar, de acuerdo con su preámbulo, el conjunto de derechos y libertades recogidos en la histórica Declaración de Derechos del Hombre y del Ciudadano de 1789, completada de acuerdo con el tenor del preámbulo de la Constitución francesa de 27 de octubre de 1946. Si bien, como ya se ha referido en el texto, el derecho fundamental a la intimidad o a la protección de datos no se recoge expresamente, el preámbulo de la Constitución francesa de 1946 proclama, como principio clave, la necesidad de que l*a Nación* proporcione *al individuo y a la familia las condiciones necesarias para su desarrollo*.
28. *Vid*. nota anterior.

las sanciones administrativas y el capítulo II establece las penales. La ley italiana de protección de datos incluye así en su articulado las penas privativas de libertad, sin incluirlas en el Código penal, tal como hemos visto que se preveía en el resto de ordenamientos. Otras vulneraciones del derecho a la intimidad sí que quedan reguladas por el Código penal, como son la inviolabilidad del domicilio y el secreto de las comunicaciones (arts. 614 y 615).

Las sanciones administrativas se regulan en los artículos 161 a 165 de la ley y el procedimiento a seguir se prevé en el artículo 166. Las multas van de los 500 a los 90.000 euros. El máximo al que puede ascender una sanción es a los 90.000 euros en el caso de que se multiplique por tres la multa prevista para los casos de vulneración del deber de información cuando se trate de datos sensibles o que presentan un riesgo específico y la multa a aplicar resulte ineficaz debido a la condición económica del infractor.

En cuanto a las sanciones penales, éstas se recogen en los artículos 167 a 172 de la ley. La pena máxima es de tres años de prisión para el que lleve a cabo una declaración o una aportación de documentos falsos.

4.5. La legislación sueca

La Constitución de Suecia de 1974 recoge en su capítulo segundo el catálogo de derechos y libertades del individuo. Concretamente, el artículo 3 garantiza la protección de los ciudadanos «contra cualquier lesión de su integridad personal resultante del almacenamiento de datos que les afecten, mediante tratamiento informático». También la inviolabilidad del domicilio y el secreto de las comunicaciones son objeto de expresa proclamación, en el artículo 6 de la Carta Magna de Suecia.

La directiva europea se traspuso en Suecia mediante la Ley de Datos Personales de 29 de abril de 1998. Los artículos 48 y 49 determinan los daños y las penas a aplicar, respectivamente.

El artículo 48 establece que el responsable de los datos personales compensará a la persona registrada por daños y por violación de la integridad personal causada por el tratamiento de datos llevado a cabo ilícitamente. Sin embargo, si prueba que el error no fue causado por él, la obligación del pago de la compensación puede verse reducida o desaparecer completamente.

El artículo 49 castiga con multa o prisión de un máximo de 6 meses o de 2 años, si la infracción es grave, a quien intencionadamente o por negligencia lleve a cabo alguna de las conductas previstas en el citado precepto. Se trata de un sistema de días-multa en el que se determina la importancia o gravedad de la misma, no por una suma de dinero, sino por un número de días, según la gravedad del delito. Cada día equivale a una concreta cantidad de dinero, según la posición económica del condenado.

El capítulo cuarto de la parte segunda del Código penal sueco lleva por título «De los crímenes contra la libertad y la paz». El artículo 9c penaliza el incumplimiento del deber de secreto de datos personales con una multa o con la pena de un máximo de dos años de prisión. La tentativa, preparación o conspiración para llevar a cabo este delito también quedarán castigadas por el Código penal, de acuerdo con el artículo 10, que remite al capítulo 23 del mismo. El capítulo 25 de la tercera parte del mismo código regula el sistema de multas.

4.6. Consideraciones finales

Las distintas leyes analizadas parten de un tronco común, la Directiva europea, si bien difieren en distintos aspectos, que pueden observarse en el siguiente cuadro comparativo:

En primer lugar, conviene reparar en las diferencias de técnica legislativa que se aprecian en los ordenamientos jurídicos estudiados, respecto de la elección entre el Código penal o la opción por una ley penal especial, para la tipificación de las conductas con relevancia penal, en materia de protección de datos.

País	Ley de Protección de Datos		Código penal
España	Arts. 44-45 Infracciones leves: 601,01 a 60.101,21 € Infracciones graves: 60.101,21 a 300.506,05 € Infracciones muy graves: 300.506,05 a 601.012,10 €		1 a 4 años prisión + multa de 12 a 24 meses – tipo básico (Art. 197.2 CP) 2 a 5 años prisión – tipo agravado 3 a 5 años prisión – tipo agravado encargado o responsable 4 a 7 años prisión– tipo hiperagravado
Alemania	Párrafo 43 Multa de 25.564 a 255.645 €	Párrafo 44 Hasta 2 años de cárcel o multa por las conductas del párrafo 43 realizadas con ánimo de lucro o con intención de perjudicar a un tercero	Párrafo 202a Espionaje de datos: pena de prisión o multa no superior a 3 años
Francia	Art. 45 a 47 Primera infracción: multa no superior a 150.000 € Infracción reiterada: multa no superior a 300.000 €		Arts. 226-16 a 226-24 Pena de prisión de 5 años + multa de 300.000 €
Italia	Arts. 161-165 De 500 a 90.000 €	Arts. 167 a 172 Penas de 3 meses a 3 años	
Suecia	Multa de 6 meses a 2 años (sistema días multa)	Art. 49 Pena de 6 meses a 2 años	

En España, las infracciones y sanciones administrativas se recogen en la LOPD, mientras que las infracciones penales y sus consecuencias se establecen en el Código penal. A diferencia de la legislación española, la norma alemana prevé infracciones y sanciones penales dentro de la misma ley de protección de datos. Además, en el Código penal alemán se recoge el delito de espionaje de datos, por lo que no todas las conductas con relevancia penal quedan tipificadas en la ley especial. En el caso de Francia, la ley de protección de datos hace expresa remisión al Código penal francés, donde encontramos las diversas conductas escogidas por el legislador para dotarlas de naturaleza delictiva, así como las penas que lleva anudada su realización. La ley italiana, por su parte, recoge todas las infracciones (también las penales) en materia de protección de datos en una única norma, no incluyendo el Código penal ninguna referencia a vulneraciones de este bien jurídico. En Suecia, por último, se recogen infracciones y sanciones punitivas tanto en una ley especial, como en el Código penal.

En segundo lugar, dentro de las sanciones administrativas y desde un punto de vista cuantitativo, también existen diferencias notables. Observamos que el importe de la sanción más elevada en Alemania es menor de la mitad de la multa prevista en España para las infracciones más graves. También en el caso francés la sanción pecuniaria es menor que en el caso español. El legislador francés prevé un máximo de 300.000 euros, cifra que se dobla en el caso del máximo español. En cuanto a Italia, nos encontramos ante el Estado Miembro con las multas menos cuantiosas de los que nos ocupan, con un máximo de 90.000 euros. España, pues, cuenta con el régimen sancionador más duro de toda la Unión Europea y ello puede colocar a las empresas españolas en una situación de desigualdad frente a sus competidores europeos. Las sanciones han sido criticadas y calificadas de desmesuradas e incluso se ha afirmado que van en contra del espíritu de la directiva, que entre sus objetivos contemplaba el de eliminar las diferencias que separaban los niveles de protección de la intimidad en los Estados Miembros para no obstaculizar el ejercicio de una serie de actividades económicas a escala europea.[29]

En tercer lugar, las penas privativas de libertad con las que se sancionan las conductas delictivas, son también dispares. En España la pena de prisión puede llegar hasta los siete años en el caso de vulneración del núcleo duro del derecho llevada a cabo con fines lucrativos. La pena prevista en el Código penal francés fija los cinco años como máximo a aplicar; es, por tanto, superior a las penas

29. A. HERRÁN ORTIZ (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Madrid: Dykinson. Pág. 357.

previstas en la norma española, a excepción del tipo hiperagravado del artículo 197.6 CP y de la agravación cualificada prevista para los encargados o responsables de los ficheros, si revelan o difunden los datos (art. 197.4 CP); asimismo, es superior a la pena prevista en el código alemán, que fija un máximo de tres años de pena privativa de libertad para quien incurra en delito. Italia se sitúa al lado de Alemania en cuanto a la pena máxima a aplicar, que no superará los tres años. Finalmente, la pena prevista en el ordenamiento sueco es inferior a los demás ordenamientos analizados, pues se establece un máximo de dos años de reclusión para quien cometa el tipo delictivo del artículo 9c, muy por debajo de los cinco años previstos en el ordenamiento francés, y también por debajo de las penas previstas en la ley española y alemana. En cuanto a la ley italiana, la pena máxima es de dos años, salvo que se lleve a cabo una declaración o una aportación de documentos falsos, en cuyo caso la pena puede elevarse hasta los tres años de prisión.

Conclusiones

El derecho a la autodeterminación informativa nace con el fin de dotar a las personas de cobertura jurídica frente a los riesgos que supone el tratamiento automatizado de datos personales.

El alcance de protección de este derecho no queda ceñido a la protección de informaciones especialmente sensibles, sino que su tutela se extiende a cualquier dato relativo a una persona que se incluya en una base de datos. Se trata de datos que pueden resultar inocuos *a priori*, pero capaces de dejar de serlo si son descontextualizados o usados para un fin completamente distinto de la finalidad para la cual fueron recabados.

La Unión Europea, consciente de que el avance de las tecnologías de la información facilita el tratamiento y el intercambio de datos, adoptó la Directiva 95/46/CE con el fin de eliminar los obstáculos a la circulación de datos y conseguir un equivalente nivel de protección de los derechos y libertades de las personas, por lo que al tratamiento de datos se refiere, en todos los Estados Miembros.[30] Dicha pretendida armonización, destinada a atajar las diferencias existentes entre las legislaciones nacionales, no se ha logrado, sin embargo, en el ámbito de las infracciones y sanciones, como hemos podido comprobar a través del análisis de algunas de estas legislaciones. La misma Unión ha reconocido esta situación de heterogeneidad legislativa en el *Informe sobre el primer Informe acerca de la implementación de la Directiva de Protección de Datos*, de 24 de febrero del 2004. La Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) fue autorizada por el Parlamento para redactar dicho informe, mientras la Comisión de Asuntos Jurídicos (JURI) y la de Industria, Investigación y Energía (ITRE) fueron consultadas para dar su opinión. En el informe, la Comisión LIBE lamenta el hecho de que la tardía implementación de la Directiva y las continuas diferencias en el modo de aplicarla hayan impedido a los operadores económicos sacar el máximo beneficio de ésta y hayan bloqueado algunas actividades (punto 6). Además, subraya que se acentúa la necesidad de que los Estados Miembros y las instituciones europeas adopten un nivel equivalente de protección de los derechos fundamentales y de los individuos en la aplicación de la Directiva (punto 22). Ambos puntos son compartidos por la Comisión JURI. La Comisión ITRE, por su parte, señala que la heterogeneidad de las diferentes leyes nacionales de protección de datos dificulta el desarrollo del mercado interior y pide a la Comisión que apoye a los Estados miembros en la interpretación y aplicación de la directiva de forma consecuente.

Por tanto, si bien el camino de la armonización de legislaciones, en cuanto a tratamiento de datos personales, parecía haber culminado con la directiva, harán falta más esfuerzos normativos para acercar las aún distantes leyes de protección de datos de los diferentes Estados Miembros.

Bibliografía

ANARTE BORRALLO, E. (2003). «Sobre los límites de la protección penal de los datos personales». En: *Derecho y conocimiento*. Huelva: Universidad de Huelva. Vol. 2, pág. 225-254.

30. *Vid*. Considerando n.º 8 de la directiva.

CAMPUZANO TOMÉ, H. (2000). *Vida Privada y Datos Personales*, Madrid: Tecnos.

CARRILLO LÓPEZ, M. (2003). *El derecho a no ser molestado*. Navarra: Aranzadi.

CASTILLO JIMÉNEZ, C. (2001). «Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información». En: *Derecho y conocimiento*. Huelva: Universidad de Huelva. Vol. 1, pág. 35-48.

COLLADO GARCÍA-LAJARA, E. (2000). *Protección de datos de carácter personal. Legislación, comentarios, concordancias y jurisprudencia*. Granada: Comares.

DAVARA RODRÍGUEZ, M. A. (1997). *Manual de derecho informático*. Pamplona: Aranzadi.

DÍEZ-PICAZO, L. M. (2003). *Sistema de derechos fundamentales*. Madrid: Civitas.

GRIMALT SERVERA, P. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Comares.

HERRÁN ORTIZ, A. I. (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Madrid: Dykinson.

LUCAS MURILLO DE LA CUEVA, P. L. (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

MARTÍNEZ MARTÍNEZ, R. (2001). *Tecnologías de la información, policía y Constitución*. Valencia: Tirant Lo Blanch.

MARTÍNEZ MARTÍNEZ, R. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Civitas.

MORALES PRATS, F. (2004). «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio». En: VARIOS AUTORES. *Comentarios al Nuevo Código Penal*. G QUINTERO OLIVARES (dir.). Thomson-Aranzadi, Navarra. 3.ª ed., pág. 1038 y sig.

REBOLLO DELGADO, L. (2005). *El derecho fundamental a la intimidad*. Madrid: Dykinson. 2.ª ed.

SÁNCHEZ, A.; SILVEIRA, H.; NAVARRO, M. (2003). *Tecnología, intimidad y sociedad democrática*. Barcelona: Icaria. 1.ª ed.

WARREN, S. D.; BRANDEIS, L. D. (1890). «The right to privacy». *Harvard Law Review*. Volumen IV, n.º 5, pág. 193-219. Traducción al castellano de BENIGNO PENDÁS y PILAR BASELGA (1995). Publicada bajo el título *Derecho a la intimidad*. Madrid: Civitas.

Cita recomendada

BRU, Elisenda (2007). «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

‹http://www.uoc.edu/idp/5/dt/esp/bru.pdf›

ISSN 1699-8154

Sobre la autora

Elisenda Bru

ebru@uoc.edu

Licenciada en Derecho (URV, 2002). Máster en Derecho ambiental (URV, 2005) y posgrado de especialización en Desarrollo humano (UOC, 2006). Su trayectoria profesional se ha desarrollado en el ámbito universitario, en el que ha trabajado como técnica de investigación en la Facultad de Ciencias Jurídicas de la URV y en la UOC, donde actualmente lleva a cabo su tarea como miembro del grupo de investigación IN3 DEUSETIC (Derecho Europeo de la Seguridad y TIC), en el marco de los Estudios de Derecho y Ciencias Políticas.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias*

Isabel García Noguera

Fecha de presentación: abril de 2007
Fecha de aceptación: junio de 2007
Fecha de publicación: septiembre 2007

Resumen
El presente trabajo pretende exponer algunas de las novedades previstas en el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código penal, presentado en el Congreso el pasado 15 de enero de 2007.[1] Concretamente, se analizarán las propuestas de reforma relacionadas con la falsificación, el tráfico y el uso ilícito de las tarjetas de crédito y débito, cuyo tratamiento jurídico-penal provoca algunas dificultades interpretativas. En efecto, el panorama actual obliga, en ocasiones, a elegir entre la impunidad que deriva de la estricta aplicación del principio de legalidad y la adaptación forzada de los tipos tradicionales a situaciones nuevas para los que no estaban realmente pensados, con el consiguiente riesgo para los principios de legalidad penal y proporcionalidad que ello puede suponer. Teniendo en cuenta que estos principios constituyen no sólo el límite extrínseco, sino también, y sobre todo, el fundamento intrínseco de la intervención penal, debe evitarse que los cambios que implican las formas emergentes de delincuencia desarrolladas en el contexto de la sociedad de la información se traduzcan en una interpretación excesivamente extensiva del tipo penal. Así, toda vez que existe un proyecto de reforma que podría aliviar estas tensiones, corresponde plantearse si la misma otorga cobertura suficiente a los supuestos de falsificación, tráfico y uso ilícito de tarjetas y si las futuras disposiciones pueden afectar a la calificación jurídico-penal de conductas como la manipulación de tarjetas auténticas o la extracción ilícita de dinero metálico en cajeros automáticos.

Palabras clave
tarjetas bancarias, estafa, falsificación, robo con fuerza, reforma penal, TIC

Tema
Derecho penal y TIC

* El contenido de este artículo coincide, en lo fundamental, con la comunicación presentada en el III Congreso de Internet, Derecho y Política (IDP). Nuevas perspectivas, organizado por los Estudios de Derecho y Ciencias Políticas de la Universitat Oberta de Catalunya (UOC). La comunicación obtuvo el primer premio *ex aequo* junto a la presentada por Elisenda Bru Cuadrada. El presente trabajo se inscribe en la actividad del Grupo de Investigación del IN3 DEUSETIC (Derecho Europeo de la Seguridad y TIC).

1. Puede accederse al documento del proyecto, que actualmente se encuentra en la última fase de su tramitación, a través de la página web del Congreso: http://www.congreso.es/.

Penal reform regarding the falsification, trafficking and illegal use of bank cards

Abstract

This work aims to disclose some of the new additions envisaged within the Draft Organic Law that is set to amend Organic Law 10/1995, dated 23 November, of the Penal Code, presented to Congress on 15 January 2007.[2] Specifically, an analysis will be carried out of the proposed reforms relating to the falsification, trafficking and illegal use of credit and debit cards, the legal-penal handling of which gives rise to certain interpretive difficulties. Indeed, the current panorama sometimes obliges us to choose between the impunity derived from the strict application of the principle of legality and the forced adaptation of traditional models to new situations for which they were never truly designed, with the subsequent risk to the principles of penal legality and proportionality that this may entail. Bearing in mind that these principles constitute not only the extrinsic limit, but also, and most importantly, the intrinsic foundation of penal intervention, the changes implied by the emerging criminal methods developed within the context of the information society must not be allowed to translate into an overly-broad interpretation of the penal type. So, whenever draft reform measures arise that may reduce such tensions, it should be considered whether the proposed measures provide sufficient protection against cases of falsification, trafficking and illegal use of bank cards, and whether future regulations may affect the legal-penal classification of such behaviour as the manipulation of authentic bank cards or the illegal withdraw of money from cash machines.

Keywords

bank cards, fraud, falsification, armed robbery, penal reform, ICT

Topic

Penal law and ICT

Introducción

Las tecnologías de la información y de la comunicación (en adelante, TIC) han abierto multiplicidad de caminos a la criminalidad[3] que, fácilmente y antes que el derecho penal, se adapta exitosamente al cambio y muta con la misma rapidez que los avances tecnológicos, cuando no los provoca, para mejorar sus técnicas criminales. Los bienes jurídicos (patrimonio, orden socioeconómico, fiabilidad del tráfico jurídico) se encuentran, pues, ante nuevos riesgos que el derecho penal debe afrontar. Ello le ocasiona numerosas tensiones, pues ultrapasar los límites trazados por el principio de legalidad con el recurso a interpretaciones extensivas o analógicas puede suponer la vulneración de la expresión máxima de la

2. You can access the project document, currently in its final processing phase, via the Congress website: http://www.congreso.es/.
3. Un amplio análisis general de las diferentes formas de criminalidad emergentes en la sociedad de la información se realiza en:
VARIOS AUTORES (2003). *Delincuencia informática. Problemas de responsabilidad*. Consejo general del poder judicial. Centro de documentación.
O. MORALES GARCÍA (dir.) (2002). *Cuadernos de Derecho Judicial, et passim*.
O. MORALES GARCÍA (2005). «Derecho penal y Sociedad de la Información». En: M. PEGUERA POCH (coord.). *Derecho y nuevas tecnologías* (págs. 417-421). Ed. UOC.
C. M. ROMEO CASABONA (coord.) (2006). *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Ed. Comares, *et passim*.
J. J. GONZÁLEZ RUS (1986). «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos». En: *Revista de la Facultad de Derecho de la Universidad Complutense*. N.º 12, págs. 107 y 108.

división de poderes en un Estado democrático de derecho y el despojo de toda justificación para la intervención penal. Ese precio será siempre más alto, incluso, que el de advertir, resignados, cómo determinadas conductas no obtienen una subsunción satisfactoria y logran deslizarse entre los espacios de impunidad. La resignación del estudioso del derecho penal deriva de la constatación de que todo proceso de adaptación del ordenamiento a nuevas realidades debe estar presidido por el dilema entre la acuciante necesidad de proteger los bienes jurídico-penales ante los nuevos ataques y el imperativo respeto al principio de legalidad penal, que impide la aplicación analógica de los tipos existentes a situaciones nuevas.[4]

Dentro de este ámbito tecnológico, la falsificación, el tráfico y uso ilícito de tarjetas de crédito y de débito sintetizan en buena medida los problemas esbozados.

1. Modalidades delictivas relacionadas con tarjetas bancarias

Desde mediados del siglo pasado, se ha ido incrementando progresivamente el uso de tarjetas bancarias, hasta convertirlas hoy en día en un medio de pago habitual,[5] lo que conlleva que también resulten uno de los objetivos preferidos de la delincuencia económica, ya sea como objeto del delito ya sea como instrumento del mismo. Siguiendo esa dicotomía objeto-instrumento, las modalidades delictivas relacionadas con las tarjetas bancarias pueden describirse y clasificarse de la siguiente manera:[6]

1.1. Conductas que tienen como *objeto* la tarjeta

- Falsificación
- Clonación
- Tráfico

En el primer supuesto, la falsificación, nos encontraríamos en sentido estricto ante la creación *ex novo* de una tarjeta falsa. A diferencia de la clonación, el falsificador no se limita a duplicar el documento copiando los datos de la banda magnética, sino que logra crear propiamente una relación crediticia nueva a través de la confección de un nuevo documento íntegramente falso. La dificultad que supone la creación de una relación crediticia ficticia explica que en la mayoría de los casos la conducta afecte principalmente a entidades bancarias que son atacadas desde dentro.[7]

La clonación (o doblaje) de tarjetas auténticas podría entenderse incluida dentro de la misma conducta que se acaba de describir, pues, siguiendo un concepto amplio de falsificación, la copia resultará siempre una falsificación respecto de la tarjeta original. De hecho, la jurisprudencia

4. Una interesante aproximación a la llamada sociedad del riesgo y a la influencia que ésta ejerce sobre el Derecho penal puede consultarse en: J. M. SILVA SANCHEZ (1999). *La expansión del Derecho penal. Aspectos de la política criminal en las Sociedades post-industriales* (págs. 22 y sig.). Ed. Civitas. B. MENDOZA BUERGO (2001). *El Derecho penal en la Sociedad del Riesgo* (págs. 44-48). Ed. Civitas. Los cambios tecnológicos y su influencia en el derecho suelen englobarse en la noción «sociedad del riesgo». Algún autor, precisamente, ha visto en la revolución tecnológica «la gran excusa para aumentar la represión sin ataduras»: G. QUINTERO OLIVARES (2004). *Adonde va el Derecho Penal* (pág. 51). Cuadernos Civitas. A. GALÁN MUÑOZ (2006). «Expansión e intensificación del Derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática». En: *Revista Aranzadi de Derecho y Proceso Penal*. N.º 15, págs. 22 y sig. Por su parte, define el «derecho penal de la Informática» como parte integrante del «moderno derecho penal» o «derecho penal del riesgo». Dentro de este concepto, los riesgos generados por el desarrollo de las sociedades postindustriales estarían motivando una respuesta penal caracterizada por una paulatina relajación de las garantías individuales, la anticipación de la intervención penal, la protección de intereses difusos y la progresiva desconfiguración de las categorías dogmáticas, aspectos todos ellos no siempre justificables desde la perspectiva de la protección del bien jurídico.
5. Para una introducción más detallada del origen y evolución del tratamiento jurídico penal de las conductas delictivas relacionadas con las tarjetas bancarias, puede consultarse: O. MORALES GARCÍA. «Derecho penal y Sociedad de la Información». En: VARIOS AUTORES. *Derecho y nuevas tecnologías. Op. cit.*, págs. 417-421. E. M. FERNÁNDEZ GARCÍA; J. LÓPEZ MORENO (1997). «La utilización indebida de tarjetas con banda magnética en el Código Penal de 1995». En: *Revista del Poder judicial*. N.º 46, págs. 569 a 572.
6. La clasificación que se realiza en la presente comunicación pretende facilitar el análisis y adecuarlo a la reforma penal en curso. Pueden consultarse distintas tipologías de casos en: O. MORALES GARCÍA. «Derecho penal y Sociedad de la Información». En: VARIOS AUTORES. *Derecho y nuevas tecnología. Op. cit.*, págs. 417-421. J. A. CHOCLAN MONTALVO. «Infracciones patrimoniales en el proceso de transferencia de datos». En: VARIOS AUTORES. *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*. C. M. ROMEO CASABONA (dir.) (2006). *Estudios de Derecho penal y Criminología* (págs. 74 y sig.). Ed. Comares. E. M. FERNÁNDEZ GARCÍA; J. LÓPEZ MORENO. «La utilización indebida de tarjetas... ». Op. cit., págs. 575 y sig. L. RAMÓN RUIZ. «Uso ilícito y falsificación de tarjetas bancarias». [Artículo en línea]. *IDP, Revista de Internet, Derecho y Política*. N.º 3. UOC [Fecha de consulta: 24/04/07] <http://www.uoc.edu/idp/3/dt/esp/ruiz.pdf>
7. A modo de ejemplo, la STS 146/2005, de 7 de febrero conoció vía casación de un caso en el que un empleado bancario «fabricaba» tarjetas para apoderarse de su crédito.

del Tribunal Supremo no ha dudado en asimilar ambas conductas,[8] otorgando el mismo tratamiento a la clonación y a la falsificación en sentido estricto, para equiparar ambas a la falsificación de moneda del art. 286 CP. Sin embargo, es importante tener presente que la relación crediticia preexistente no se modifica, ya que sólo se ha clonado el soporte material que la contiene, por lo que no nos encontramos ante situaciones idénticas. Ello comporta importantes repercusiones para la calificación jurídico-penal como más adelante se tendrá ocasión de observar.[9] Por lo demás, las tarjetas auténticas habrán sido normalmente sustraídas a su titular por la comisión de un hurto o robo o de cualquier otro modo ilícito, por lo que en la mayoría de casos se estará frente a un concurso de delitos, pero también puede suceder que se trate de tarjetas extraviadas.

Por lo que se refiere al tráfico de tarjetas bancarias, lo normal será que tal conducta se anude a la actividad de organizaciones criminales a media o gran escala. Éstas suelen actuar en distintos países aprovechando los espacios de impunidad que los llamados «paraísos jurídicos» les proporcionan a nivel internacional.[10]

1.2. Conductas que tienen la tarjeta como instrumento (uso ilícito de tarjetas o de los datos contenidos en ellas)

- Extracción ilegítima de dinero metálico en cajeros automáticos.
- Adquisición ilegítima de bienes o servicios por el uso de tarjetas en terminales de puntos de venta.
- Pago no consentido a través de redes informáticas.

En realidad, todas estas conductas serían reconducibles a la categoría más amplia de «uso ilícito de tarjetas o de los datos contenidos en ellas». En esta categoría, donde la tarjeta es el instrumento y no el objeto de la acción, la casuística es más variada y compleja, por lo que se ha procedido a seleccionar para el presente análisis los supuestos más relevantes. Los más comunes son las extracciones de dinero en cajeros automáticos, en los que el sujeto activo utiliza la tarjeta para acceder a la máquina que, una vez tecleado el número secreto, pondrá a su disposición la cantidad de dinero solicitada.[11] El segundo supuesto lo constituye la adquisición de bienes o servicios simulando ser el titular de la tarjeta ante el terminal de un punto de venta comercial. Puede mediar engaño al dependiente del establecimiento comercial pero puede que éste actúe en connivencia con el sujeto activo.[12] El último de los supuestos que analizaremos contempla la utilización en Internet de los datos contenidos en la misma para la obtención a distancia de bienes o servicios.[13]

2. Regulación vigente

Para abordar el tratamiento jurídico-penal que reciben las conductas que se acaban de enumerar, se partirá de la clasificación anterior. Asimismo, se tomarán como referencia los tipos concurrentes aparentemente aplicables para ir descartándolos o no en función de su adecuación a las conductas objeto de análisis.

8. SSTS 948/2002 de 8 de julio y 1680/2003, de 11 de diciembre.
9. *Vid.* nota 17.
10. Sobre la denominación «paraísos informáticos» *vid*. D. K. PIGAROFF. «Presentation of the Draft United Nations Manual on Prosecution and Prevention of Computer Crime». En: U. SIEBER (ed.) (1994). *Information Technology Crime*. Pág. 609. Colonia, Bonn, Munich: V. Carl Heymanns. A. GALÁN MUÑOZ. «Expansión e intensificación del Derecho penal de las nuevas tecnologías...». *Op. cit.,* pág. 20.
11. La escasa probabilidad estadística de acertar la combinación numérica requerida, ha conducido a un intenso debate doctrinal acerca del carácter relativo o absolutamente inidóneo de la tentativa en los casos en los que se ha intentado hacer uso de la tarjeta sin conocer el número secreto. Los márgenes de este trabajo impiden abordar en profundidad tales aspectos, pero puede consultarse la siguiente bibliografía: SILVA; MORALES; CASABONA. Aunque resulte difícil negar la concurrencia ex ante de un cierto riesgo para el bien jurídico, podría cuestionarse el carácter de «suficiente» del riesgo generado para entender punibles estos supuestos de tentativa. A pesar de la impunidad que podría derivarse al considerar estos «intentos» como absolutamente inidóneos (pues, de hecho, es matemáticamente posible acertar, por azar, con la clave de acceso durante los tres intentos que habitualmente permite el cajero automático), parece conveniente diferenciar entre lo «matemáticamente posible» y lo que deba entenderse por «probabilidad de riesgo relevante» para el bien jurídico protegido. En todo caso, parece necesario examinar caso por caso para evaluar el nivel de riesgo desarrollado por la conducta *ex ante*, pues, en ocasiones, el sujeto activo podría no tener el conocimiento efectivo de la contraseña pero sí conocer otros datos de la víctima (su fecha de nacimiento, por ejemplo) que facilitasen el descubrimiento de la clave. En tales supuestos, como puede fácilmente inferirse, la probabilidad de acierto dejaría de ser remota y la tentativa, paralelamente, resultaría punible. En similares términos se pronunció la SAP de Las Palmas de 17 de enero del 2004 al entender que, pese a que el acierto del número secreto es «estadísticamente despreciable y prácticamente irrealizable», debía apreciarse la tentativa punible en el caso concreto, pues los sustractores de la tarjeta tenían acceso al número secreto guardado en el monedero que le habían sustraído a la víctima.
12. O incluso puede tratarse de la misma persona que simula las operaciones mercantiles. *Vid*., por ejemplo, la STS de 26 de junio 2006.

2.1. Calificación jurídico-penal de la falsificación de tarjetas

Como ya se tuvo ocasión de aclarar, tanto la tarjeta falsa creada *ex novo* como la tarjeta fruto de la clonación de otra auténtica pueden ser entendidas como resultados de la misma acción de falsificación. Lo mismo cabe decir de la manipulación de alguno de los elementos (nombre, firma, etc.) de una tarjeta auténtica con el fin de adecuarlos a su nuevo e ilegítimo poseedor. Por esta razón se utilizará el término *falsificación* en un sentido amplio para aludir a todos estos supuestos, aunque no sean idénticos y, por lo tanto, no tengan por qué recibir el mismo tratamiento jurídico-penal.

2.1.1. La falsificación de tarjetas y los delitos de falsedad en documento mercantil y de falsificación de moneda

Con anterioridad al Código penal de 1995, la falsificación de tarjeta se reconducía generalmente a la falsedad en documento mercantil,[14] si bien resultaba complicado incluir las bandas magnéticas en el concepto de documento del Código penal de 1973.[15]

El Código penal de 1995 contribuyó a la solución de algunos problemas que afectaban a esta materia, pero también, paradójicamente, a complicar el problema de su subsunción. Este doble efecto se entiende por la introducción, por una parte, de un concepto amplio de documento en la redacción del actual art. 26 CP, que hizo menos conflictiva la inclusión de las bandas magnéticas en el concepto de documento. Pero, junto a esta previsión, se introdujo como novedad en el art. 287 CP la asimilación de las tarjetas bancarias a la moneda, a los efectos del delito de falsificación de moneda (art. 286 CP).[16]

La primera cuestión, en relación con dicha asimilación, fue dilucidar, dentro de todas las modalidades posibles de manipulación de tarjetas bancarias, qué conductas debían circunscribirse dentro de la acción de falsificar, y ser por ello calificadas de falsificación de moneda, y cuáles debían seguir siendo calificadas como falsedad en documento mercantil. No es asunto baladí, pues, la inclusión de cualquier manipulación falsaria dentro del art. 286 CP comporta una pena de 8 a 12 años de prisión, frente a la de 6 meses a 3 años que se prevé para la falsedad en documento mercantil (arts. 390 y 392 CP). La Sala Segunda del Tribunal Supremo zanjó la cuestión por medio del Acuerdo no jurisdiccional de 28 de junio de 2001, en el que se

13. Se dejan fuera del presente análisis varias conductas: el abuso de crédito por parte del titular legítimo de la tarjeta, la simulación de solvencia para obtener crédito de entidades bancarias, colocación de instrumentos de clonación informática de tarjetas en los cajeros automáticos, etc. Estos supuestos son convenientemente analizados por otros trabajos: J. A. CHOCLAN MONTALVO, «Infracciones patrimoniales...». *Op. cit., págs.* 87 y 88. E. M. FERNÁNDEZ GARCÍA; J. LÓPEZ MORENO, «La utilización indebida de tarjetas...». *Op. cit*., págs. 575 y sig. L. RAMÓN RUIZ, «Uso ilícito y falsificación...». *Op. cit., págs.* 6 y 7. Baste aquí indicar que los dos primeros supuestos no parecen plantear problemas de subsunción en la estafa básica del art. 248.1 CP, siempre y cuando se emplee un engaño suficiente para crear el error en la entidad bancaria, pues de lo contrario habría de acudirse al incumplimiento contractual por vía civil. El último supuesto, por su parte, podría constituir una tentativa de las modalidades falsarias que se analizan más adelante en el presente trabajo.
14. En ese sentido: E. BACIGALUPO ZAPATER. «Documentos electrónicos y delitos de falsedad documental». En: VARIOS AUTORES. *Delincuencia informática. Problemas de responsabilidad*. O. MORALES GARCÍA (dir.) (2002). *Servicio de Formación Continuada, Escuela Judicial*. Pág. 3. Alude también a la problemática: E. M. FERNÁNDEZ GARCÍA; J. LÓPEZ MORENO. «La utilización indebida de tarjetas...». *Op. cit.*, pág. 587. Secundan esta línea doctrinal: SSTS 3 de diciembre de 1991 y 15 de marzo de 1994.
15. En general, sobre el concepto de documento y otros aspectos relativos a la falsedad documental interesa consultar: C. VILLACAMPA ESTIARTE (1999). *La falsedad documental. Análisis jurídico-penal*. Cedecs, *et passim*. Con relación a las dificultades que tenían lugar con anterioridad al concepto amplio de documento introducido en el art. 26 por el CP de 1995, C. M. ROMEO CASABONA (1988). «Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos». En: *Poder Judicial*. N.º 9 (esp.), pág. 123. Los datos, al estar cifrados informáticamente en las bandas magnéticas, no eran susceptibles de ser aprehendidos directamente por el ser humano, por lo que no podían integrar el concepto penal de documento anclado, con anterioridad al CP de 1995, en el paradigma cartáceo También la perdurabilidad de los datos informáticos planteaba problemas en este sentido. En consecuencia, el último autor citado sostuvo que cuando la conducta falsaria recayese sobre la banda magnética, ésta debía entenderse atípica.
16. Por otro lado, la exclusión de los particulares de la órbita del sujeto activo en la comisión de las falsedades ideológicas ha venido a complicar el panorama de las falsedades documentales en general, lo que incrementa, de forma refleja, los problemas de calificación de la falsificación de tarjetas bancarias. G. QUINTERO OLIVARES. «De las falsedades documentales». En: VARIOS AUTORES. *Comentarios al Nuevo Código Penal*. G. QUINTERO OLIVARES (Dir.) (1975/1977). 3.ª ed., págs. 1975-1977.

declaró que «la incorporación a la «banda magnética» de uno de estos instrumentos de pago, de unos datos obtenidos fraudulentamente, constituye un proceso de fabricación o elaboración que debe ser incardinado en el art. 386 del Código penal». Una vez asentada tan categórica doctrina, ya no podría sólo asimilarse a la falsificación de moneda la creación de una tarjeta falsa, único supuesto comparable a la «creación de dinero nuevo»,[17] sino que todas aquellas conductas que impliquen la introducción de datos fraudulentos en la tarjeta (falsa o auténtica) deberían reconducirse a la falsificación de moneda.

Como se ha encargado de poner de relieve gran parte de la doctrina, la asimilación que realiza la Sala Segunda implica graves consecuencias para el principio de proporcionalidad de las penas.[18] Aunque en algún caso concreto la manipulación de tarjeta pudiera dar lugar a un desvalor equiparable al de falsificación de moneda, debe advertirse que generalmente (y en la abstracción de la norma es donde debe iniciarse el juicio de proporcionalidad) la pena resultará desproporcionada. Simplemente porque no tiene la misma repercusión en el tráfico la introducción de dinero falso, que el aprovechamiento fraudulento de una relación crediticia preexistente a la manipulación de la tarjeta.[19] A mayor abundamiento, como la falsificación de tarjetas se acompaña normalmente de su uso ilícito, habrá de hacerse concursar el delito de falsificación de moneda con el delito patrimonial de que se trate, lo que lógicamente elevará la pena por aplicación de las reglas concursales.[20]

Frente a los problemas de subsunción que, a continuación veremos, se suscitan con ocasión del uso ilegítimo de tarjetas, la falsificación de tarjetas no ofrecería, pues, problemas desde la pura perspectiva de la seguridad jurídica. A tenor de lo dictado por la Sala Segunda, la calificación para todos los supuestos ha de ser la de falsificación de moneda. Sin embargo, la certeza puede resultar acaso más indeseable que la incertidumbre, cuando se cobra tan alto precio a costa del principio de proporcionalidad de las penas.

2.2. Calificación jurídico-penal del uso ilícito de tarjetas bancarias

El uso ilícito de tarjetas bancarias se caracteriza tanto por la variedad en sus modos de perpetración como en la pluralidad de sus posibles calificaciones jurídicas, lo que suele plantear problemas de seguridad jurídica. Vaya, pues, por delante el aviso de que no se va a llegar a soluciones consensuadas y que los tipos penales que se barajan como posibles calificaciones para estos supuestos son la estafa básica del art. 248.1 CP, el fraude informático del art. 248.2 CP y el robo con fuerza en las cosas de los arts. 237 y 239 CP. Aunque la proliferación de tipos a aplicar pudiera dar a entender que las conductas se encuentran contempladas desde varios flancos o sobreprotegidas, se trata de una torpe ilusión. La realidad es que pueden subsistir importantes espacios de impunidad y que los bienes jurídicos en juego también pueden sufrir una correlativa desprotección.

2.2.1. Uso ilícito de tarjetas y estafa «clásica» del art. 248 CP

Este tipo defraudatorio, tal y como la doctrina penal española mayoritaria ha señalado reiteradamente,[21] requiere la concatenación causal de los siguientes elementos: un

17. L. RAMÓN RUIZ. «Uso ilícito y falsificación...». *Op. cit*., pág. 5.
18. E. M. FERNÁNDEZ GARCÍA; J. LÓPEZ MORENO. «La utilización indebida de tarjetas...». *Op. cit*., págs. 590 y 591.
19. En la conducta de falsificación de tarjeta, la creación del documento falso supone a su vez la creación de una relación crediticia ficticia. No sucede lo mismo cuando se procede a la duplicación o clonación de una tarjeta auténtica sin alterar la relación crediticia legítima existente. Por lo tanto, sólo la falsificación (en sentido estricto) podría asimilarse propiamente a la falsificación de moneda, resultando excesiva la misma calificación penal para la clonación de tarjetas, aunque en un sentido más laxo del término puedan entenderse como falsificaciones. Es lo que ya se ha querido poner de relieve *supra* al definir las conductas de falsificación y clonación de tarjetas en el apartado dedicado a la descripción de las modalidades delictivas relacionadas con tarjetas bancarias. Así lo ha sostenido: O. MORALES GARCÍA. «Derecho penal y Sociedad de la Información». En: VARIOS AUTORES. *Derecho y nuevas tecnologías. Op. cit.,* pág. 420.
20. STS de 8 de julio de 2002: «Hay que recordar que (...) la alteración de la banda magnética, que supone la generación de una tarjeta *ex novo*, integra, por sí misma, el delito de falsificación de moneda, independiente del uso posterior fraudulento a que ese instrumento de pago mendaz pueda ser destinado, produciéndose, en tal caso, una relación concursal entre ambos ilícitos»
21. La bibliografía es, naturalmente, extensísima. *Vid*. por todos: J. M. VALLE MUÑIZ. «De las defraudaciones». En: VARIOS AUTORES. *Comentarios al Nuevo Código Penal. Op.cit.*, págs. 128 y sig. C. CONDE-PUMPIDO FERREIRO (1997). *Estafas.* Págs 26 y sig. Ed. Tirant lo Blanch.

engaño bastante que cree un error en la víctima, de tal manera que ésta realice un acto de disposición patrimonial en perjuicio propio o de tercero. Por su propia estructura parece necesaria una relación *intuitu personae* entre el estafador y la víctima, que no concurre en la mayoría de los supuestos que aquí examinamos, donde la acción irá casi siempre referida a un sistema o dispositivo informático (un ordenador, un cajero automático, un datáfono...).[22] La única excepción a esta dinámica sería el uso de tarjetas en terminales de puntos de venta, puesto que el uso de la tecnología resulta en estos casos casi anecdótico. Por esta razón, no parece complicado aplicar la estafa básica a estas situaciones, siempre y cuando el encargado de pasar la tarjeta por el datáfono no esté en connivencia con el sujeto activo y pueda hablarse con propiedad de la concurrencia de engaño y error.[23] Finalmente, debería descartarse la subsunción en el delito básico de estafa de la compraventa a través de Internet, pues la mayor parte de la doctrina coincide en señalar que no hay modo de acomodar una relación a distancia, y que se efectúa a través de medios informáticos, a la relación interpersonal entre el estafador y el estafado que se proyecta desde el art. 248.1 CP. Con todo, debe analizarse caso por caso el nivel de automatización de la transacción, pues en ocasiones puede constatarse la existencia de alguna relación o comunicación entre el comprador y el vendedor que posibilitaría apreciar una relación interpersonal susceptible de encajar en la estafa básica.[24]

2.2.2. Uso ilícito de tarjetas y fraude informático del art. 248.2 CP

El Código penal de 1995 incluyó en el segundo apartado del art. 248 CP la conducta de quien, a través de manipulación informática o artificio semejante, realice una transferencia de un activo patrimonial en perjuicio de tercero. A pesar de la concepción mayoritariamente personalista de la estafa «clásica» regulada en el primer apartado del art. 248 CP, el sujeto activo del fraude informático previsto en el segundo apartado de dicho precepto «también se considera reo de estafa»,[25] cuando quizás lo más apropiado hubiese sido reservar tal denominación para los supuestos defraudatorios interpersonales tradicionales. La elección de la creación de un tipo defraudatorio específico desvinculado de la estafa del tipo básico y caracterizado por la instrumentación de una manipulación informática o artificio semejante, podría evitar gran parte de las confusiones que actualmente se producen con ocasión de las tensas relaciones entre el tipo básico y, como algunos autores las denominan de forma significativa, las estafas «impropias».[26]

22. En cualquier caso, no son supuestos en los que exista un elemento intelectual susceptible de sufrir un error. *Vid*., en este sentido, O. MORALES GARCÍA. «Malversación, estafa informática y falsedad en documento electrónico. Algunas reflexiones sobre la STS de 30 de octubre de 1998». En: VARIOS AUTORES. *El nuevo Derecho penal. Estudios penales en memoria del profesor José Manuel Valle Muñiz*. G. QUINTERO OLIVARES; F. MORALES PRATS (Coord.) (2001). Págs. 1565 a 1606. Ed. Aranzadi.
«En Alemania, recuerda MORALES GARCÍA, igualmente, la discusión sobre el alcance del artículo 263 StGB, que regula la estafa tradicional, en relación con las manipulaciones informáticas encerraba problemas jurídicos de diversa índole (...) limitadas al ámbito del engaño (*Tauschung*) y el error de la víctima (*Irrtum des Opfers*). Es decir, es imposible inducir a error al ordenador, pues, paradójicamente, se le induce a actuar correctamente conforme a los parámetros introducidos en el sistema.» (pág.1591).
23. Es menester señalar cómo el deber de diligencia exigido en la comprobación de la identidad del comprador parece haber elevado las cotas del engaño para poder ser tenido por suficiente, pudiéndose pensar en caso contrario que nos encontramos frente en una situación de autopuesta en peligro, falta de cuidado que no tendría que ser subsanada por la actuación del sistema penal. Sobre la suficiencia del engaño, por citar una de las sentencias más recientes: STS de 2 de febrero de 2007.
24. L. R. RAMÓN RUIZ. «Uso ilícito y falsificación de tarjetas bancarias». *Op. cit*., pág. 7. El autor trae a colación la SAP de Baleares de 15-10-2004, que, si bien en un principio señala la posibilidad de aplicar el tipo de estafa básica a un supuesto de compra venta fraudulenta por Internet a través de tarjeta de tercero, lo acaba descartando por no poderse apreciar un engaño idóneo dado el deber de vigilancia que había sido desatendido por el vendedor. De un modo similar resuelve la SAP de Málaga de 17 de febrero del 2006.
25. El legislador penal de 1995 quiso, probablemente, remarcar la pertenencia del nuevo tipo a los delitos defraudatorios y diferenciarlo de los delitos patrimoniales de naturaleza apropiatoria como el hurto o el robo. Pero el Tribunal Supremo ha partido siempre de «un plano subjetivo (en el que) han de tenerse en cuenta las especiales condiciones del sujeto pasivo, cociente intelectual, situaciones personales de mayor sugestionalidad, edad, etc.», STS de 28 de noviembre del 2002. Del mismo modo, para la suficiencia del engaño se ha acudido siempre a la diligencia del hombre medio que se ve «sorprendida por el ardid empleado por el sujeto activo de forma que los mecanismos de defensa desplegados por el sujeto pasivo no capten la mendacidad del artificio empleado y produzcan error en el mismo», STS 778/ 2002 de 6 de mayo.
26. C. CONDE-PUMPIDO FERREIRO. *Estafas. Op. cit.,* págs. 205 y sig.

Debe ponerse en duda, en todo caso, que el fraude informático recoja el desvalor propio de todas las modalidades de uso ilícito de tarjetas de crédito y de débito.[27] Piénsese que en los supuestos que estamos analizando se procede a la introducción de datos correctos en un sistema informático que funciona correctamente, de manera que difícilmente podrá hablarse de la manipulación informática o el artificio semejante[28] que requiere el art. 248.2 CP. Por manipulación informática debe entenderse toda modificación del resultado de un proceso automatizado de datos, mediante la alteración de los mismos, «en cualquiera de las fases de su procesamiento o tratamiento informático».[29] Mayores dudas de interpretación suscita la noción de artificio semejante, cuya significación tanto podría referirse a otro tipo de artimañas informáticas distintas de la estricta manipulación (por ejemplo, la introducción de programas espía –*spyware*– para averiguar una clave), como a otro tipo de maniobras sobre el sistema relacionadas con la tecnología aunque no integren el sentido espiritual de la manipulación informática.[30] Esta última interpretación, con todo, parece demasiado amplia, permitiendo la inclusión en el art. 248.2 CP de, por ejemplo, las modificaciones materiales sobre el hardware para alterar el funcionamiento de la máquina con finalidad defraudatoria, lo que parece alejarse bastante de la teleología del fraude informático.[31] Pero, ni aun con la interpretación más extensiva posible del concepto de artificio semejante, podremos hacerle abrazar lo que no resulta sino su antónimo: la normalidad del sistema.

Abundando en esta cuestión, algunos autores llaman la atención sobre casos en los que sería discutible sostener que el sistema funciona normalmente. Según afirman, el art. 248.2 CP sí que podría ser de aplicación en aquellos casos en los que se manipulase la tarjeta (supuestos de falsificación o clonación), puesto que en estos casos sí que podría hablarse de manipulación informática o el artificio semejante.[32]

No se comparte aquí la misma opinión. Si se sostiene que el tipo defraudatorio del art. 248.2 CP recoge todo el desvalor de la conducta, debemos preguntarnos si la manipulación a la que hace referencia el tipo está pensada para la falsificación de tarjetas.[33] Efectivamente, no puede dejar de hacerse notar que, para encajar en el tipo, la falsificación (tenida por manipulación o artificio semejante) debería verse completada causalmente por una conducta posterior de transferencia de activos patrimoniales. Sin esa ultractividad, el tipo no se vería completo, y no porque se discuta que se trate de un supuesto de tentativa, sino porque en realidad no nos encontramos ante una dinámica defraudatoria incompleta, sino ante una conducta falsaria consumada. La manipulación de la tarjeta es una conducta distinta del uso posterior que del instrumento falsificado se haga. Apreciar una tentativa de fraude informático en supuestos de manipulación de tarjeta equivaldría a seccionar el tipo penal, desfigurándolo y desarrollando una labor *cuasi* legislativa que no nos corresponde. En definitiva, el legislador configuró la infracción para criminalizar determinadas transferencias ilegítimas de activos patrimoniales aprovechando la flexibilidad que brinda la tecnología, pero no para conductas falsarias que posterior-

27. En sentido afirmativo: E. BACIGALUPO ZAPATER (1988). «Utilización abusiva de cajeros automáticos por terceros no autorizados». En: *Poder Judicial*. N.º 9 (esp.), págs. 87 y sig. J. A. CHOCLAN MONTALVO. «Infracciones patrimoniales...». *Op. cit*., pág. 85. Para estos autores, la elasticidad de la cláusula extensiva del «artificio semejante» resulta suficiente para englobar distintas modalidades de uso ilícito de tarjetas, como la extracción de dinero metálico en cajeros automáticos.
28. J. A. CHOCLAN MONTALVO. «Infracciones patrimoniales...». *Op. cit*., pág. 85. El autor descarta la hipótesis de la manipulación pero no totalmente la del artificio semejante, dada su amplitud.
29. C. M. ROMEO CASABONA (1988). *Poder Informático y seguridad jurídica*. Pág. 47. Ed. Fundesco.
30. El peligro de la laxitud del término se observa en algunas sentencias, como la STS 26 de junio del 2006, que llega a definir el artificio semejante como «artimaña, doblez o truco», confundiendo el fraude informático con la estafa tradicional.
31. En ese sentido: J. M. VALLE MUÑIZ. «De las defraudaciones». *Op. cit*., pág. 1233. O. MORALES GARCÍA. «*Derecho penal y Sociedad de la Información*». En: VARUIOS AUTORES. *Derecho y nuevas tecnologías. Op. cit*., pág. 416.
32. C. CONDE-PUMPIDO FERREIRO. *Estafas. Op. cit.*, pág. 220. O. MORALES GARCÍA. «Derecho penal y Sociedad de la Información». En: VARIOS AUTORES. *Derecho y nuevas tecnologías. Op. cit*., pág. 420.
33. STS de 8 de julio de 2002: «las bandas magnéticas (...) constituyen, en sí, un soporte material cuya alteración supone un acto distinto de las meras operaciones o manipulaciones informáticas para conseguir la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, que, por ejemplo, se produciría cuando directamente se interfiriera en un sistema, tal como el de una entidad bancaria o en redes como Internet, para la obtención del lucro».

mente se instrumentalicen para la comisión de un fraude u otro delito patrimonial.[34]

En el caso de uso de tarjeta en cajeros automáticos, la mayoría de las veces no se producirá una transferencia de activos patrimoniales como requiere el delito del art. 248.2 CP, sino una extracción de dinero metálico o, al menos, un intento de extracción, si se retoma el debate *supra* apuntado sobre la idoneidad o inidoneidad de la tentativa en aquellos supuestos en los que el sujeto activo desconoce el número secreto. Ello no ha impedido que un sector de la doctrina defienda que el término *transferencia* debe ser interpretado en un sentido amplio, de manera que abarque tanto una determinada cantidad de dinero en efectivo, como un activo patrimonial, permitiéndose la subsunción en el tipo de fraude informático.[35]

Quizás pueda convenirse que el problema no reside tanto en la diversidad de objeto (activo patrimonial versus cantidad material dineraria) como la diferencia en la acción. No parece que se haya acudido al término transferencia para describir genéricamente traspasos de un patrimonio a otro, esto es, de la órbita patrimonial del titular a la del sujeto activo de delito. Al contrario, parece más correcto afirmar que el legislador ha prefigurado el tipo del art. 248.2 CP para determinadas defraudaciones informáticas que no coinciden con la acción de las extracciones de dinero en cajeros automáticos[36] y que guardan mayor relación con los delitos apropiatorios, como podremos comprobar en el apartado siguiente.

2.2.3.Uso ilícito de tarjetas y robo con fuerza en las cosas

La naturaleza apropiatoria del delito de robo con fuerza en las cosas podría poner en duda su idoneidad para el tratamiento de delitos relacionados con las TIC, pero, en puridad, constituye la muestra de que a veces sí es posible adaptar los tipos penales clásicos a los modos comisivos más evolucionados, pues tal es la calificación que la doctrina y la jurisprudencia mayoritarias han asignado a las extracciones ilícitas de dinero en cajeros automáticos.[37]

Con todo, el esfuerzo realizado para tal adaptación puso a prueba la elasticidad del principio de legalidad durante la vigencia del CP de 1973.[38] En efecto, el Tribunal Supremo consideró[39] ya entonces que las tarjetas debían estimarse llaves a efectos del robo con fuerza, criterio que después obtuvo respaldo legislativo a través del art. 239 del Código penal de 1995.

Este entendimiento no es unánime en la doctrina, ni siquiera tras la inclusión de las tarjetas magnéticas en el concepto de

34. Debe diferenciarse el acto de falsificación del uso ilícito posterior que del documento falso se haga. Un planteamiento similar fue sostenido por Bacigalupo con ocasión de la diferenciación entre la unidad de plan y la unidad de acción para calificar separadamente la apropiación ilícita de la tarjeta de su uso ilícito posterior, en supuestos de extracción de dinero en cajeros automáticos. *Vid.* en ese sentido: E. BACIGALUPO ZAPATER. «Utilización abusiva de cajeros automáticos...». *Op. cit.*, pág. 87. De este modo discrepaba el autor del parecer expresado por la Fiscalía General del Estado en su Memoria de 1987, donde se argumentaba que la apropiación de la tarjeta y su uso ilícito posterior en cajeros automáticos respondían a una misma unidad de acción, por lo que ambas conductas debían ser globalmente calificadas en función del modo en que había sido sustraída la tarjeta (generalmente, robo con fuerza en las cosas).
35. C. CONDE-PUMPIDO FERREIRO. *Estafas. Op. cit.,* pág. 222. M. PÉREZ MANZANO. «Las defraudaciones (I). Las estafas». En: VARIOS AUTORES. *Compendio de Derecho penal (Parte Especial).* M. BAJO FERNÁNDEZ (dir.) (1998). Vol. II, pág. 456. Ed. Centro de Estudios Ramón Areces. En contra: J. M. VALLE MUÑIZ. «De las defraudaciones». *Op. cit.,* pág. 1233. O. MORALES GARCÍA. «Derecho penal y Sociedad de la Información». En: VARIOS AUTORES. *Derecho y nuevas tecnologías. Op. cit.*, págs. 415 y 416.
36. En este sentido: «la dinámica comisiva no se aparta de la clásica de apoderamiento, si bien con la peculiaridad del necesario uso de tarjeta magnética de crédito para poder acceder al objeto material del delito. No se trata, por tanto, de transferencias de activos patrimoniales, sino de sustracción de dinero mediante el uso por un tercero del medio específico adecuado para acceder al mismo. El supuesto carecía de atributos para ser reconducido al delito de estafa (con anterioridad a la entrada en vigor del nuevo Código penal), y se aleja también ahora de las conductas penalmente relevantes a título de fraude informático. Antes bien, normalmente procederá su incriminación a título de robo con fuerza en las cosas». J. M. VALLE MUÑIZ. «De las defraudaciones». *Op. cit.,* pág. 1233.
37. J. M. VALLE MUÑIZ, «De las defraudaciones» *op. cit.,* pág. 490. En contra: C. CONDE-PUMPIDO FERREIRO, *Estafas, op. cit.,* pág. 222.
38. C. M. ROMEO CASABONA (1996). «Delitos informáticos de carácter patrimonial» en *Informática y Derecho.* N.º 9, págs. 413-415.
39. STS de 16 de marzo de 1999: «el concepto de llave no es rigurosamente semántico o literal, sino funcional (...) habiéndose destacado (...) que si bien las tarjetas de crédito no son llaves en el puro sentido morfológico de la expresión, lo son en el aspecto funcional en cuanto sirven en la práctica para accionar el cierre del local que da acceso al Cajero automático o para abrir el receptáculo del mismo cuando está situado en el exterior».

llave falsa, y no faltan quienes entienden que el robo con fuerza no se adapta a todas las modalidades de extracción de dinero metálico en cajeros automáticos.[40] Concretamente, se sostiene desde esta posición que, para los supuestos en los que la tarjeta hubiese sido falsificada o manipulada, sería preferible aplicar el fraude informático del art. 248.2. CP.[41] Así, si la tarjeta fuese falsa estaríamos ante una manipulación y, por consiguiente, una defraudación, mientras que la obtención de dinero con la tarjeta auténtica pero sustraída o hallada, e indebidamente utilizada por quien no es titular, se consideraría un robo con fuerza en las cosas. Tal solución no parece ser del todo coherente, pues la calificación jurídica de conductas idénticas no puede variar en función de un dato contingente como el origen auténtico o inauténtico de la tarjeta. La jurisprudencia del TS vendría, asimismo, a corroborar este punto de vista, cuando sostiene que no cabe aplicar el tipo de estafa informática a estos casos, pues ni la extracción material de dinero se corresponde con una transferencia, ni puede apreciarse manipulación informática o artificio semejante.[42]

Otro sector de la doctrina ha resaltado, en relación con la calificación jurídica del uso de tarjetas legítimas para la extracción no consentida de dinero en cajeros automáticos, que tampoco el robo con fuerza resulta aplicable a estos casos y que resulta menos forzado acudir a la figura defraudatoria del art. 248.2 CP. Ello es así, se aduce, porque debe diferenciarse la voluntad del deseo y advertir que la extracción de dinero no se produce contra la voluntad del dueño, como reclama el art. 239 CP, sino en contra de su deseo. Dicho de otro modo, la voluntad del titular de la tarjeta es que a través de ella se pueda extraer dinero del cajero, aunque no sea su deseo que un tercero no legitimado lo haga.[43]

Finalmente, hay que tener en cuenta que existen otras formas de extracción ilícita de dinero en cajeros en las que sí que se produce una manipulación informática y una subsiguiente transferencia de activos patrimoniales, por lo que podrán subsumirse en el tipo del fraude informático. Son supuestos en los que no se hace mero y normal uso de la tarjeta, sino, por ejemplo, se procede a descifrar, por medio de algún programa informático, el número secreto del titular de la cuenta, para acceder a sus activos y realizar con ellos operaciones no consentidas.[44] Estas conductas, precisamente por no consistir en el apoderamiento material del objeto y por instrumentalizarse a través de alguna manipulación informática o artificio semejante, sí que podrían encuadrarse en el art. 248.2 CP.

3. El proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Reformas en materia de conductas relacionadas con tarjetas bancarias

Una de las características de la reforma penal emprendida por el Gobierno en julio de 2006[45] es la búsqueda de una mejor adaptación de la legislación penal a las

40. C. CONDE-PUMPIDO FERREIRO. *Doctrina y Jurisprudencia.* Vol. II, pág. 2685. Ed. Trivium.
41. C. CONDE-PUMPIDO FERREIRO. *Doctrina y Jurisprudencia. Op. cit., ibidem.*
42. STS 16 de marzo 1999*:* «con relación al nuevo art. 248.2 del texto penal vigente de 1995, hay que entender que dicho fraude informático no contempla la sustracción de dinero a través de la utilización no autorizada de tarjetas magnéticas (...) porque la dinámica comisiva no parece alejada de la clásica de apoderamiento, (...) presenta la peculiaridad de la exigencia del uso de la tarjeta magnética para poder acceder al objeto material del delito». En el mismo sentido: STS 26 de diciembre de 2000, con relación al art. 248.2 CP: «exige en su redacción la realización de actos de manipulación informática o artificio semejante, elemento de la acción que no concurre cuando lo que se realiza es un apoderamiento de dinero mediante empleo de una tarjeta válida y el número secreto correspondiente, sin ninguna manipulación informática, sino mediante el empleo de una llave- último párrafo del art. 239 del CP- sustraída a su titular».
43. Inició la doctrina Bacigalupo en su conocido voto particular a la STS de 8 de mayo 1992. La sigue: J. A. CHOCLAN MONTALVO. «Infracciones patrimoniales...». *Op. cit.,* págs. 82 *y 83.* Ambos autores prefieren hacer uso de la elasticidad del término «artificio semejante» para incluir en el art. 248.2 CP los supuestos de extracción de dinero metálico en cajeros automáticos.
44. E. ORTS BERENGUER; M. ROIG TORRES (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática.* Pág 67. Ed. Tirant lo Blanch.
45. En abril de 2005, la Sección Especial para la Elaboración de una Propuesta de Anteproyecto, compuesta por seis vocales expertos en derecho penal, inició el estudio y redacción de la propuesta en el seno de la Comisión General de Codificación. Con fecha de 14 de julio del 2006 fue aprobado en Consejo de Ministros el Anteproyecto de Ley Orgánica de Modificación de Código Penal, propuesta que pasó a ser formalmente Proyecto de Ley Orgánica el 15 de enero del presente año. La reforma abarca varios e importantes sectores de la legislación penal: desde la reincidencia o la responsabilidad penal de las personas jurídicas a aspectos de Parte especial como los que aquí se tratan, entre otros.

formas emergentes de criminalidad. Ello se refleja con especial intensidad en materia de falsificación, tráfico y uso ilícito de tarjetas bancarias, cuya regulación contiene, como hemos podido observar, algunas insuficiencias. La propuesta de reforma dedicada a esta materia ha seguido la línea trazada por la Unión Europea en la Decisión marco de 28 de mayo de 2001,[46] con el objetivo de procurar, a través de la armonización de las legislaciones penales de los Estados Miembros, una protección penal coherente con el carácter generalmente transnacional de la delincuencia económica y asociada a las TIC.[47]

El texto original de la propuesta se ha visto puntualmente modificado por las sugerencias que el Consejo General del Poder Judicial (CGPJ, en adelante) realizó en su informe aprobado el 27 de octubre de 2006.[48]

3.1. Falsificación, tráfico y uso de tarjetas falsificadas

El proyecto de reforma introduce importantes novedades en relación con las conductas objeto de estudio, añadiendo una sección 3.ª bis al capítulo II del título XVIII del libro II bajo el nombre *De la falsificación de tarjetas de crédito y débito y cheques de viaje*. Dentro de esta sección se recoge el art. 399 bis que en su primer apartado prevé la pena de 4 a 8 años de prisión para el que «falsificare, copiándolos o reproduciéndolos, tarjetas de crédito o débito o cheques de viaje». En el segundo apartado se incrimina «la tenencia de tarjetas de crédito o débito o cheques de viaje falsificados en cantidad que permita suponer están destinados a la distribución o al tráfico», conducta que prevé la misma pena que para la falsificación. Ya en el tercer inciso, el art. 399 bis tipifica la conducta del «que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados» anudándole una pena privativa de libertad de dos a cinco años. Junto a la nueva incriminación de estas conductas, debe resaltarse que se ha abandonado la equiparación de la tarjeta a la moneda a los efectos del art. 286 CP (falsificación de moneda), puesto que la nueva redacción propuesta para el art. 387 CP deja de contemplarlas. Así, con la introducción del art. 399 bis y la eliminación de las tarjetas del art. 387 CP, puede preverse que la reforma pondrá fin a la incómoda y criticada situación actual caracteri-

46. Decisión marco del Consejo de Ministros de la Unión Europea para la lucha contra el fraude en los medios de pago distintos del efectivo (2001/413/JAI). Otras acciones han sido emprendidas en el seno de la Unión Europea. En 1998, la Comisión encargó a un comité de expertos el estudio COMCRIME, iniciativa que provenía a su vez del Consejo Europeo en el marco del programa de acción relativo a la delincuencia organizada. Puede consultarse la siguiente web oficial: http://europa.eu.int/scadplus/leg/es/lvb/l33193b.htm. No puede dejar de mencionarse la Convención del Consejo de Europa sobre Cybercrimen, firmada en Budapest el 23 de noviembre del 2001. Se trata extensamente el tema en: O. MORALES GARCÍA (2002). «Apuntes de Política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre delincuencia informática». En: *Cuadernos de Derecho judicial*. N.º 9, págs. 11-34. Recientemente, se ha hecho pública una comunicación de la Comisión Europea dónde se plasma la necesidad de definir más decididamente una política europea específica en materia de lucha contra el cybercrimen. La Comisión advierte del aumento creciente de la criminalidad relacionada con las TIC y de la correlativa necesidad de coordinar las respectivas Políticas Criminales de los Estados miembro a través de Convenios y Decisiones Marco del tercer pilar. El documento, «Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. Towards a general policy on the fight against cyber crime», {SEC(2007) 641} {SEC(2007) 642}, COM/2007/0267 final, puede consultarse en la siguiente dirección: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:HTML
47. *Vid*., entre otros: U. SIEBER (1992). *The International Emergence of Criminal Information Law*. Págs. 73-99.Colonia: Carl Heymanns Verlag KG. O. MORALES GARCÍA. «Derecho penal y Sociedad de la Información». En: VARIOS AUTORES. *Derecho y nuevas tecnologías. Op. cit.,* págs. 387-470. J. J. GONZÁLEZ RUS. «Aproximación al tratamiento penal de los ilícitos...». *Op. cit.,* pág. 109. R. M. MATA MARTIN (2003). «Criminalidad informática: una introducción al cibercrimen». *Actualidad penal*. N.º 3, págs. 939-942. Algunos autores afirman, con razón, que el principal problema al que se enfrenta la delincuencia relacionada con las TIC es el conflicto de jurisdicción: R. FERNÁNDEZ PALMA (2004). «El principio de territorialidad penal y la delincuencia relacionada con las tecnologías de la información y comunicación. Comentario al auto del Juzgado de Instrucción N.º 18 de Barcelona, de fecha 5 de mayo de 2003». En*: Revista Aranzadi de Derecho y Nuevas Tecnologías*. N.º 4, págs. 127-140.
48. En realidad, la única modificación que se ha introducido en el proyecto de reforma penal a raíz de los consejos emitidos por el CGPJ en su informe, es la concerniente a la inclusión del perjuicio patrimonial de tercero en la estafa cometida a través de tarjetas bancarias, introducida por la propuesta en el art. 248.2 CP. *Vid. infra* nota 51. Puede accederse al texto del informe en la página oficial del CGPJ: http://www.poderjudicial.es/eversuite/GetRecords?Template=cgpj/cgpj/principal.htm

zada por la desproporción de la respuesta penal frente a la falsificación de tarjeta bancaria.

No por esperada debe dejar de estimarse acertada la decisión de otorgarle a la falsificación de tarjetas un tratamiento penal más proporcionado y ajustado a los presupuestos de nuestro sistema. La ubicación sistemática del art. 399 bis dentro de las falsedades documentales resulta congruente con el carácter documental que se le había reconocido a las tarjetas. La mayor penalidad asignada respecto del resto de falsedades documentales también tiene sentido vista la especial importancia de estos medios de pago en el tráfico. El tipo propuesto podría considerarse, en consecuencia, como un subtipo agravado de falsedad documental.

En similares términos de aprobación se ha pronunciado el CGPJ, si bien ha criticado otros aspectos de la regulación propuesta para la falsificación, tráfico y uso de tarjetas falsificadas.

El núcleo central de la crítica realizada por el CGPJ reside en la exclusión del primer apartado del art. 399 bis (falsificación de tarjetas) del supuesto de manipulación de tarjetas auténticas, desvinculándose del art. 2 b) de la Decisión marco de 28 de mayo de 2001.[49] Asimismo, el CGPJ critica la estrechez del segundo apartado del mismo precepto (tráfico y receptación), pues alega que no es necesario exigir una determinada cantidad de tarjetas para suponer el destino a tráfico y que la mera tenencia de una tarjeta falsa para un posterior uso fraudulento debería ser suficiente para completar la tipicidad. El tercer apartado del precepto es, sin embargo, aceptado favorablemente por el CGPJ, que lo menciona como ejemplo de seguimiento de la citada Decisión marco.

No se comparte aquí exactamente el mismo punto de vista. El CGPJ ha criticado que la reforma no incluya la manipulación de tarjetas auténticas en la noción de falsificación, pero lo cierto es que de la lectura del precepto propuesto no tiene por qué derivarse esa exclusión necesariamente. Al contrario, teniendo en cuenta la doctrina de la Sala Segunda, que asimila la manipulación de tarjeta auténtica (clonación) a la creación de una tarjeta falsa, no sería en absoluto impensable que se incluyese la misma conducta en el futuro delito de falsificación de tarjeta. De todos modos, es de esperar que para los supuestos de manipulación de tarjetas auténticas se recurra a la calificación subsidiaria de falsedad en documento mercantil, cuya menor penalidad parece más acorde con el también menor reproche que merece la manipulación frente a la creación *ex novo* de la tarjeta.

En coherencia con lo ya dicho, la descripción del art. 399 bis, sólo se referiría al tráfico de tarjetas falsas en sentido estricto, por lo que cuando se trafique con tarjetas auténticas (manipuladas o no), deberá recurrirse al tipo general de receptación (arts. 298 y sig. CP). Aunque parece que nos encontramos ante conductas similares, podría pensarse que la diferencia de trato se basa quizá en una mayor peligrosidad y dañosidad del tráfico de tarjetas falsas.

Otro tanto cabe predicar del distinto régimen previsto para el uso de tarjetas bancarias en función de si éstas son auténticas o no. Si el uso ilícito se realiza a través de tarjeta falsa acudiremos al art. 399 bis, pues se trata de una conducta asociada a la falsificación que afecta a la fiabilidad del tráfico mercantil, y si la tarjeta es auténtica, recurriremos al tipo defraudatorio del art. 248.2 c) previsto por la reforma. Ello es lógico, ya que el uso afecta en este caso exclusivamente al patrimonio del titular de la tarjeta auténtica.

Por lo que se refiere al carácter estrecho del segundo apartado del art. 399 bis, no cabe duda de que la Decisión marco de 28 de mayo del 2001 establece la incriminación de determinados actos de tráfico, incluida la "posesión de instrumentos de pago que hayan sido objeto de robo u otra forma de apropiación indebida, falsificación o manipulación, para su utilización fraudulenta". Una perspectiva maximalista del art. 2c) de la Decisión marco conduciría probablemente a la conclusión de que no se han tipificado todas las conductas relacionadas con el tráfico y uso fraudulento de tarjetas, ya que, como dice el CGPJ, no se contempla la tenencia de una sola tarjeta falsificada. Sin embargo, deberíamos preguntarnos si la directriz europea (que no es norma directamente vinculante) no

49. Se prevé que los Estados adoptarán medidas necesarias para criminalizar (...) «b) (la) falsificación o manipulación de instrumentos de pago, para su utilización fraudulenta».

estará en realidad otorgando un margen discrecional especialmente amplio a los Estados para la incriminación de estas conductas, como por otra parte viene siendo costumbre en las técnicas normativas indirectas de la Unión Europea.[50] No parece que de la utilización de la expresión «posesión de instrumentos de pago» haya de derivarse la necesaria criminalización de la tenencia de una sola tarjeta falsificada.

Debe añadirse que el informe redactado por la Comisión Europea para evaluar la adaptación de las legislaciones de los Estados Miembros a la Decisión marco no menciona que el Estado español haya cometido ningún error al respecto, como sí que se encargó de remarcar con ocasión de la manipulación de las tarjetas auténticas.[51] Simplemente se ha seguido, dentro del legítimo margen de discrecionalidad, la lógica de los principios de *ultima ratio* y fragmentariedad del Derecho penal. Desde esta otra perspectiva, el segundo inciso del art. 399 bis más bien peca de exceso de amplitud que de estrechez, pues recurre a la difusa fórmula de «en cantidad que permita suponer», expresión que podría poner en entredicho el principio de taxatividad y cuya concreción deberá realizarse jurisprudencialmente, caso de ser aprobada la reforma. Sería lógico pensar que esta modalidad seguirá la misma suerte que el antiguo delito de tenencia de moneda falsa (art. 287 CP 1973).[52] La jurisprudencia exigió un requisito valorativo o subjetivo que permitiese determinar que la tenencia estaba destinada al tráfico o la expendición, modo éste de intentar apartar el tipo de la órbita de los delitos de sospecha.[53]

3.2. El uso ilícito de tarjetas auténticas

Como decíamos, la reforma prevé la introducción de un nuevo tipo defraudatorio añadiendo un nuevo apartado tercero al art. 248.2 CP. De este modo, junto al fraude informático, se tipifica una nueva modalidad de defraudación asimilada a la estafa cometida a través de tarjetas bancarias auténticas. El precepto considera también reos de estafa a los que «utilizando tarjetas de crédito o débito, o cheques de viaje o los datos obrantes en ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de tercero». La referencia al «perjuicio a tercero» no figuraba en la versión originaria del anteproyecto, pero fue añadida con posterioridad por recomendación del CGPJ.[54]

El informe del CGPJ frente a la propuesta de un nuevo tipo de estafa hace hincapié en el carácter superfluo de la previsión, puesto que entiende que la estafa básica del art. 248.1 CP ya se ocupa adecuadamente de estos supuestos, siendo la única salvedad la de tener que apreciar un especial deber de diligencia que relativiza el carácter «bastante» del engaño. Sin embargo, como se ha evidenciado, la calificación jurídico-penal de los casos de connivencia entre el comprador y el vendedor para simular operaciones mercantiles empleando un datáfono, así como los de comercio electrónico a través de Internet, por la introducción no consentida de los datos contenidos en tarjeta ajena, no resulta satisfactoria para un amplio sector de la doctrina. Por ello, no debería adjetivarse como superflua tan fácilmente la previsión de un nuevo tipo de estafa para incriminar el uso ilícito de tarjetas auténticas, pues se estaría dando cobertura a supuestos cuya subsunción en el delito actual de estafa no resulta pacífica en la doctrina.

50. F. MORALES PRATS (1999). «Los modelos de unificación del Derecho penal en la Unión Europea: Reflexiones a propósito del "Corpus Iuris"». En: *Revista Penal*. N.º 3, págs. 29 y sig.
51. Informe de la Comisión basado en el artículo 14 de la Decisión marco del Consejo de 28 de mayo de 2001 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo {SEC(2004) 532}. Puede accederse al documento a través de la siguiente dirección electrónica: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=COMfinal&an_doc=2004&nu_doc=346&lg=es
52. En él se tipificaba la tenencia de moneda falsa cuando «por su número y condiciones se infiera racionalmente que estén destinadas a la expendición». Como se ve, la estructura es casi idéntica a la del precepto propuesto por la reforma para la criminalización de la tenencia de tarjetas falsas.
53. C. VILLACAMPA ESTIARTE. «De la falsificación de moneda y efectos timbrados». En: VARIOS AUTORES. *Comentarios al Nuevo Código Penal. Op. cit.*, pág. 1957.
54. El CGPJ apuntó con acierto «que el perjuicio recaiga sobre el "titular" de la tarjeta, excluye innecesariamente el supuesto en que la perjudicada sea la entidad emisora cuando así proceda conforme a las cláusulas contractuales, por lo que el alcance del perjuicio debería extenderse a los terceros».

Ahora bien, cabe preguntarse si la introducción de esta nueva modalidad de estafa o del tercer inciso del art. 399 bis para el uso de tarjetas falsificadas podría modificar a su vez la calificación de robo con fuerza en las cosas que las extracciones ilícitas en cajeros automáticos reciben actualmente. En buena lógica, no parece que dicha calificación pueda variarse por la introducción de un nuevo tipo defraudatorio dado que la jurisprudencia y la doctrina mayoritarias están de acuerdo en distinguir una naturaleza apropiatoria en la dinámica de estas conductas que difícilmente podrán encajar en una modalidad defraudatoria, por mucho que ésta se instrumente por medio de tarjeta bancaria, aunque lo cierto es que formalmente cabría en la fórmula amplia prevista por el prelegislador.

Lo mismo debería predicarse de las nuevas previsiones para el uso ilícito de tarjetas falsas. Si bien la letra del art. 399 bis parece englobar todo uso de tarjeta falsa, el criterio de especialidad dicta que la calificación de un concreto uso de tarjeta falsa, la extracción de dinero en cajeros automáticos, ha de dirigirse igualmente al tipo de robo con fuerza. La especialidad debe, pues, en este caso, referirse a la dinámica comisiva y no al tipo de tarjeta que se utilice, porque es aquélla la que realmente determina el ataque sobre el bien jurídico protegido (apropiación patrimonial a través de llave falsa) y no el carácter falsario del medio empleado. A pesar de que el uso de tarjetas falsas reciba un tratamiento diferente en atención al bien jurídico protegido en los tipos falsarios, no debe perderse de vista que el uso no entraña propiamente la falsificación. Se asocia a la falsificación de forma instrumental pero no comparte su naturaleza, pues no es un fin en sí mismo. Es necesario contemplar la posibilidad de que el uso de tarjeta falsa se materialice en un concreto perjuicio patrimonial cuya dinámica encaje mejor en el robo con fuerza en las cosas.

Comparando las penalidades de los respectivos tipos, debe concluirse que en el tercer apartado del art. 399 bis el legislador ha reservado un reproche mayor, de dos a cinco años de prisión, para conductas más graves que las contempladas en el robo con fuerza, castigado con una pena de uno a tres años de prisión. La diferencia punitiva tiene sentido en el entendimiento de que el uso de tarjetas falsas describe un doble ataque (patrimonial y falsario), pero si el ataque es simple (sólo patrimonial) el uso de la tarjeta falsa para la extracción de dinero en cajeros automáticos no colmaría todo el desvalor contemplado por el tipo. La conducta debería, en definitiva, valorarse al margen del carácter auténtico o inauténtico de la tarjeta utilizada, y ello porque ha de seguirse el mismo razonamiento esgrimido para el debate sobre si la falsificación de una tarjeta podía integrar o no la manipulación informática o artificio semejante del fraude del art. 248.2 CP.[55] El Tribunal Supremo ya se pronunció en sentido negativo, por lo que cabe esperar que siga la misma línea y mantenga la calificación de robo con fuerza en las cosas para estos supuestos.

Naturalmente, habrá de atenderse a la aplicación judicial y al desarrollo doctrinal que de la reforma pueda hacerse, caso de ser finalmente aprobada, para el desarrollo de conclusiones y propuestas más depuradas o definitivas.

Cita recomendada

GARCÍA NOGUERA, Isabel (2007). «La reforma penal de la falsificación, tráfico y uso ilícito de las tarjetas bancarias». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

<http://www.uoc.edu/idp/5/dt/esp/garcia.pdf>

ISSN 1699-8154

55. *Vid. supra* notas 28 y 30.

Sobre la autora

Isabel García Noguera

igarcian@uoc.edu

Licenciada en Derecho (UAB, 2002), diploma de Estudios Avanzados en Sociedad de la Información y el Conocimiento (UOC, 2006). Su trayectoria profesional se inicia en el ámbito de la investigación como asistente de investigación en el proyecto E-Crime (2002-2003), y el inicio del doctorado interuniversitario «Empresa y sistema penal», en el marco del Instituto Joan Lluís Vives. Su perfil se complementa en el campo de la docencia con la realización de consultorías en las asignaturas de Derecho penitenciario, Criminología y Derecho penal II (UOC, 2003-2005 y 2007). Actualmente, elabora su tesis en el campo de la delincuencia informática a nivel europeo bajo la dirección de la Dra. Fernández Palma y es miembro del área jurídica del proyecto Le-sig y del grupo de investigación IN3 DEUSETIC.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

Crónica

Consejo de redacción de la revista IDP

El Congreso Internet, Derecho y Política –celebrado en Barcelona los días 7 y 8 de mayo del 2007– llegó a la tercera edición con el objetivo de continuar la tarea de reflexión, análisis y discusión de las principales transformaciones del derecho y de la política en la sociedad de la información. El III Congreso se centró en las cuestiones que en el momento de su celebración constituían los retos y novedades más relevantes en los campos del *copyright*, la protección de datos, la seguridad en la red, los problemas de responsabilidad, el voto electrónico y la regulación de la administración electrónica, además de dedicar un espacio específico al estado del uso de las TIC por parte de los profesionales del derecho. El III Congreso IDP ofreció a los profesionales, académicos y personas interesadas, un espacio de debate y de información, tanto científica como práctica, de las perspectivas que se avistaban en los ámbitos mencionados.

Este Congreso es impulsado por los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya en el marco del IN3 (Internet Interdisciplinary Institute), instituto que reúne toda la actividad de investigación que se lleva a cabo en la UOC y que centra su ámbito principalmente en el estudio de los efectos de las tecnologías de la información y la comunicación en las personas, las organizaciones y la sociedad en general.

La conferencia inaugural (*keynote speech*) del Congreso fue a cargo del profesor Jonathan Zittrain, del Oxford Internet Institute, con el título «The future of the Internet and how to stop it». El profesor Zittrain hizo un repaso a la evolución de los programas de ordenadores a lo largo de la historia. Desde sus inicios, cuando el software formaba parte integrante (e inseparable) del hardware, pasando por la separación en la producción y distribución de software y hardware que hizo posible la expansión y éxito de Internet, hasta los programas de última generación, los llamados web 2.0, que hacen posible una mayor independencia y flexibilidad por parte del usuario en la utilización del software. Ahora bien, independencia y flexibilidad comportan una mayor sensación de inseguridad y de peligro para los otros usuarios del software: cuanta más independencia se tiene en el software que utilizamos para actuar en Internet, más inseguridad en términos de protección de la intimidad, los datos personales, etc. El profesor Zittrain nos advirtió del peligro que corre el futuro de los nuevos programas de ordenador, a raíz de esta sensación de inseguridad en Internet y de la demanda de mayor seguridad de los usuarios: el retorno de la integración de software y hardware como medio para ofrecer una mayor seguridad en el tráfico en Internet.

El segundo panel de la mañana estuvo dedicado a la responsabilidad de los proveedores de servicios de Internet por los contenidos alojados en la red. Los ponentes fueron la profesora Lilian Edwards, de la Facultad de Derecho de la Universidad de Southampton, y el profesor Miquel Peguera, de los Estudios de Derecho y Ciencia Política de la UOC. La profesora Edwards, en una ponencia titulada «From Censorship to Cartelisation? ISP Control of Illegal and Harmful Content», expuso los resultados de un estudio sobre los sistemas de notificación y retirada de contenidos en el Reino Unido. El profesor Peguera analizó las tendencias jurisprudenciales en la aplicación de las normas de la Ley de Servicios de la Sociedad de la Información, que excluyen la responsabilidad de los intermediarios por los contenidos ilícitos procedentes de terceros. Moderó la sesión la profesora Raquel Xalabarder, de los Estudios de Derecho y Ciencia Política de la UOC.

La última sesión de la mañana, moderada por Esther Mitjans, directora de la Agencia Catalana de Protección de Datos, se dedicó a las perspectivas del derecho fundamental respecto a la protección de datos. El catedrático de Derecho Constitucional y magistrado del Tribunal Supremo, Pablo Lucas, puso de manifiesto que

el reto del ordenamiento jurídico español en materia de protección de datos era el de aplicar las normas de carácter general en sectores que representaban particularidades especialmente complejas y necesitadas de una regulación singular, y que se entraba en una nueva etapa en la que había que defender el derecho a la protección de datos de carácter personal con los medios jurídicos de que se disponía, cuya solución adecuada, con el fin de garantizar este derecho, era tanto la intervención pública, como la actuación privada, dirigiendo e impulsando la primera en la segunda.

Por su parte, el profesor Yves Poullet, director del Centre de Recherche en Informatique et Droit de la FUNDP, puso el acento en que los sistemas de información se estaban convirtiendo en omnipresentes como consecuencia de la multifuncionalidad de los equipos terminales de telecomunicaciones y de la creciente conexión entre redes, así como de la necesidad de nuevos principios con el fin de proteger adecuadamente al ciudadano en el nuevo entorno tecnológico.

Propuso cinco nuevos principios: el de encriptación y anonimato reversible, el de beneficios recíprocos, el de potenciación de soluciones tecnológicas que favorecieran y no fueran en contra de la privacidad, el del completo control por parte del usuario del equipo terminal y el principio según el cual los usuarios de determinados sistemas de información pudieran beneficiarse de la legislación sobre defensa de los consumidores y usuarios.

El profesor Poullet afirmó la necesidad de hacer extensivos los deberes de protección de datos a otros sujetos que hasta el momento no eran contemplados por la legislación: los productores de software y de terminales que tendrían que informar al usuario de los riesgos de utilizar las redes y que tendrían que velar para que los productos fabricados garantizaran una mayor protección de la privacidad.

Esta sesión la cerró Ricard Martínez, profesor de Derecho constitucional de la Universitat Oberta de Catalunya y coordinador de los Estudios del AEPD, que incidió en la necesidad de un nuevo marco legal que diera respuesta a la profunda transformación tecnológica en un marco donde el consumidor es totalmente frágil y no tiene una cultura de protección de datos. En esta nueva sociedad vigilada, la existencia de autoridades de control constituye una de las garantías básicas para poder controlar la información personal.

La tarde se inició con una sesión dedicada al debate y reflexión sobre cuestiones penales relacionadas con los procesos de transferencia de datos (seguridad en la red). Contamos con dos ponentes de diferente trayectoria y experiencia. Ramón García Albero, catedrático de Derecho Penal de la Universidad de Lérida, centró su ponencia en la influencia que las TIC, y otros elementos que caracterizan a la actual sociedad, están promoviendo en el entendimiento y alcance de los principios básicos que fundamentan y legitiman el derecho penal. Advirtió de la laxitud con que ya se están aplicando las categorías penales y de su traducción en tipos punitivos, en los cuales es difícil detectar un bien jurídico directamente protegido (pornografía virtual, accesos acondicionados, etc.).

Antonio López, inspector del Cuerpo Nacional de Policía y oficial de enlace en Europol, intervino con la ponencia «Investigaciones en Internet: estructuras de cooperación policial internacional», exponiendo el impacto que las tecnologías de la comunicación y la información significaban para la delincuencia; la repercusión de éstas en la operatividad de los sistemas clásicos de investigación criminal; la reacción del ordenamiento jurídico ante la insuficiencia de las técnicas tradicionales, y las estrategias más avanzadas, desde el punto de vista policial y de cooperación internacional, en la lucha contra este sector de la delincuencia. Especialmente interesante resultó el relato del *iter* de la investigación policial de algunos casos reales de especial complejidad, así como el debate suscitado en torno a los diferentes puntos de vista sostenidos por los conferenciantes.

La mesa redonda sobre «Las nuevas fronteras del copyright» fue a cargo del profesor John Palfrey, director ejecutivo del Berkman Center for Law & the Internet, y del profesor Jonathan Zittrain, del Oxford Internet Institute, bajo la moderación del profesor Ramon Casas, profesor titular de Derecho civil en la Universidad de Barcelona. Los ponentes, con la ayuda del público asistente, examinaron las circunstancias y las posibles justificaciones y defensas jurídicas de las partes, en la demanda que Viacom planteó contra Google por las infracciones de propiedad intelectual que los usuarios cometen al cargar ciertos contenidos en Youtube sin la autorización de sus titulares. Las circunstancias concretas de este caso sirvieron para exa-

minar el sistema de límites (el *fair use* en Estados Unidos, o la copia privada, la información de actualidad y la parodia en España), que podrían justificar las acciones en Youtube y, en caso de no ser así, la posible responsabilidad de Google por las infracciones cometidas por sus usuarios: ¿hasta qué punto Google es responsable de las infracciones de propiedad intelectual que se cometen en sus portales?

La segunda jornada del Congreso se inició con una sesión dedicada al voto electrónico. El voto electrónico ya es una realidad en varios países del mundo, y en España y Cataluña se han llevado a cabo ya numerosas pruebas piloto. No obstante, las reticencias hacia las votaciones electrónicas son muy fuertes por todas partes y se han criticado diferentes aspectos de estos procedimientos, como la eliminación del acto simbólico y cívico de la presencialidad del voto, los fallos de los sistemas de seguridad y la falta de culturización de la población ante estos sistemas.

En la mesa redonda contamos con dos especialistas en voto electrónico, Josep Maria Reniu, profesor de Ciencia política de la UB y colaborador docente de la UOC, y Gerard Cervelló, pre-sales manager de SCYTL, empresa puntera y exportadora de sistemas de voto electrónico. La mesa estuvo moderada por la profesora de los Estudios de Derecho y Ciencias Políticas, Rosa Borge, experta en participación electrónica. Ambos ponentes explicaron los diferentes sistemas de voto electrónico más habituales y los países donde se utilizaban, además de los problemas que se podían producir. El debate se centró también en los temas de seguridad y en los cambios legislativos que necesitan los sistemas de votación electrónica.

A continuación, tuvo lugar la ponencia dedicada a la Ley de Administración Electrónica. El director general de Modernización Administrativa del Ministerio de Administraciones Públicas presentó los contenidos principales del Proyecto de Ley de Acceso Electrónico de los Ciudadanos a las Administraciones Públicas, que en aquel momento estaba en tramitación parlamentaria. Asimismo, explicó las diferentes fases que se han seguido para la elaboración del mencionado texto.

A continuación, el Dr. Julián Valero, profesor de Derecho administrativo de la Universidad de Murcia, hizo una lectura del texto del proyecto de ley valorando la necesidad de una regulación de la administración electrónica y destacando tanto las principales novedades, como aquellos elementos más problemáticos o algunas de las carencias que presentaba el proyecto de ley. La sesión suscitó interesantes cuestiones por parte del público.

En paralelo a estas dos sesiones de la mañana, tuvo lugar una jornada profesional que constituyó una novedad de la 3.ª edición del Congreso IDP. La finalidad de estas jornadas, de un fuerte carácter profesionalizador, es la reflexión, el debate y la discusión sobre las problemáticas y realidades de colectivos concretos. La jornada en el marco del III Congreso se dedicó a la protección de datos en la Universidad e iba dirigida a todos los profesionales responsables o técnicos de la protección de datos en este ámbito, al mismo tiempo que planteaba cuestiones de utilidad para todo el sector educativo. Esta jornada contó con la colaboración de la Agencia Catalana de Protección de Datos (APDCAT), que, en la persona de su directora, inauguró la jornada.

Ricard Martínez estructuró su intervención desmontado los mitos que normalmente giran en torno a la protección de datos: la implementación de una política de protección de datos parece imposible e inalcanzable y comporta costes inasumibles. Indicó como principales objetivos los de identificar a quién tiene que tratar los datos, detectó las necesidades del usuario y publicó un protocolo de protección de datos. Concluyó indicando que la adopción de una política de seguridad por parte de las universidades no sólo es indispensable por el hecho de que está en juego un derecho fundamental y las universidades tienen que ser pioneras en su defensa, sino también por el hecho de que los datos (la información) constituyen uno de los activos de la Universidad y como tal hay que protegerlos.

Por su parte, Eugenio Fernández, director de Sistemas de Información de la Universidad Rey Juan Carlos, redundó en la necesidad de tener una política de seguridad informática y la conveniencia de que haya alguna persona u órgano que dirija todas las políticas de seguridad y que en definitiva responda a las cuestiones respecto a cuáles son los datos que se tratan, cómo se tratan y cuándo se pueden tratar.

Posteriormente, tuvo lugar un vivo debate moderado por Maite Casado, responsable del Área de Inspección del APDCAT.

La última sesión del III Congreso IDP consistió en una mesa redonda sobre el uso de las tecnologías entre los profesionales del derecho, moderada por el profesor Pere Fabra, director de los Estudios de Derecho y Ciencia Política de la UOC. La Dra. Marta Poblet, investigadora del Instituto de Derecho y Tecnología de la Universidad Autónoma de Barcelona, expuso los resultados de un estudio sobre los usos de las tecnologías de la información por parte de los abogados, y las tendencias que se observan en este ámbito. El Sr. Pere Lluís Huguet, decano del Colegio de Abogados de Reus y presidente del Consejo de los Ilustres Colegios de Abogados de Cataluña, habló sobre las mejoras impulsadas por el uso de las nuevas tecnologías por parte de los abogados. El Dr. Luis Fernández del Pozo, registrador mercantil de Barcelona, y el notario Miquel Roca Bermúdez de Castro expusieron el estado del uso de las nuevas tecnologías en los campos registral y notarial.

Acto seguido se entregó el Premio a la Mejor Comunicación Presentada al Congreso, que se concedió *ex aequo* a Elisenda Bru e Isabel García, becarias de doctorado del IN3.

Esta 3.ª edición del Congreso IDP representó la consolidación de éste como plataforma para la reflexión y el estudio que los constantes cambios y transformaciones de las tecnologías de la información y comunicación comportan para la sociedad, y los retos que surgen constantemente para el derecho y la ciencia política.

IDP. Revista de Internet, Derecho y Política es una publicación electrónica semestral impulsada por los Estudios de Derecho y Ciencia Política de la UOC, que tiene como objetivo la comunicación y divulgación científica de trabajos de análisis e investigación sobre los retos y cuestiones que las tecnologías de la información y la comunicación plantean con respecto al derecho y la ciencia política.

IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA. N.º 5 (2007).

EDITA: Gabinet de Comunicació. Publicacions a Internet. **DIRECCIÓN:** Dani Martí. **EDICIÓN EJECUTIVA:** Lluís Rius. **COORDINACIÓN EDITORIAL:** Maria Boixadera. **ASISTENTE DE EDICIÓN:** Margarita Perelló. **CORRECCIÓN Y TRADUCCIÓN DE TEXTOS:** Clara Ortega, Jonathan Rushton, Nita Sáenz, Rut Vidal (Eureca Media, SL). **MAQUETACIÓN:** Maria Abad (Eureca Media, SL). **PROGRAMACIÓN WEB:** Elena Coronas, Diego Fernández, Gonzalo García, Carlos Lavatelli (Eureca Media, SL). **DISEÑO:** Elogia y Grafime. **ISSN:** 1699-8154. **DEPÓSITO LEGAL:** B-29.619-2005. **DIRECCIÓN POSTAL:** Universitat Oberta de Catalunya. Avda. Tibidabo, n.º 39-43. 08035 Barcelona. **DIRECCIÓN ELECTRÓNICA:** idp@uoc.edu. **WEB IDP:** http://idp.uoc.edu/

UOC
Universitat Oberta de Catalunya
www.uoc.edu