CAPÍTULO TERCERO

LA INTIMIDAD

CAPÍTULO TERCERO

LA INTIMIDAD

I. LA INTIMIDAD EN LA ENCRUCIJADA

El derecho a la intimidad requiere una especial consideración en un trabajo de este tipo por la intensa amenaza que para el mismo supone Internet. La Red no sólo es un nuevo medio de comunicación, sino que también se configura como un nuevo medio de vigilancia. Presenta un potencial para agredir a la intimidad sin precedentes, que exige que el poder público muestre una atención prioritaria por estas cuestiones. Aparece un verdadero "reto para los derechos de privacidad" (Rosenoer, 1997, 141). El Estado, como indica Álvarez-Cienfuegos (1999, 14) debe asumir una posición beligerante en la defensa de los derechos de la persona, y permanecer ajeno a la "tensión dialéctica entre consumo de información y defensa de la personalidad". La jurisprudencia ha afirmado que "el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas han obligado a extender (la) protección" de la vida privada (Sentencia del Tribunal Constitucional español 110/1984). La doctrina, a su vez, se muestra unánime a la hora de subrayar el potencial peligro a que se ve sometida la intimidad con el desarrollo de las nuevas tecnologías. Al mismo tiempo, se recogen afirmaciones ciertamente preocupantes que consideran inevitables las agresiones a la intimidad ("derechos básicos como la intimidad desaparecen" —Tapscott en Cebrián, 1998, 21—).

Los peligros que amenazan a la intimidad desde Internet provienen tanto del aparato estatal como de particulares, lo que constituye una afirmación tan rotunda que pide a

gritos mecanismos de defensa que hagan eficaz la protección horizontal del derecho (*Drittwirkung*) y no sólo frente a las agresiones del poder público. Dicho esto es preciso añadir algo más para ilustrar correctamente la cuestión: Internet supone nuevas amenazas para la intimidad y, al mismo tiempo, ofrece nuevas vías de protección. Es un ejemplo paradigmático de las contradicciones de la propia Red. Internet, sin duda, "está llena de contradicciones" (Hick/Halpin/Hoskins, 2000, 187).

Con demasiada habitualidad se perciben distintas disfunciones en las redes informáticas que han provocado cierta intranquilidad al mostrarse más inseguras de lo que algunos pensaban. Sirvan de ejemplos la saturación de ciertos servidores de Estados Unidos (*Yahoo, Amazon, eBay* o la CNN) por el fenómeno que se conoce como *mail bombing*; el espionaje que Estados Unidos y Gran Bretaña llevan a cabo en Europa a través de la organización Echelon;* el centro de control de correo electrónico del servicio de contraespionaje británico del M15; el sistema informático que está desarrollando el gobierno estadounidense de control de comunicaciones, Total Information Awareness System (que permitirá rastrear millones de bases de datos mediante cruces de las mismas); el sistema diseñado por el FBI de seguimiento, análisis y descifrado del correo electrónico, *Carnivore* (que es capaz de realizar un análisis sintáctico y de expresiones para detectar "actitudes contrarias a la ley"); o los problemas de seguridad de alguna empresa de telefonía; al margen de los periódicos cuadros de pánico debido a un nuevo y presuntamente catastrófico

* Esta red, nacida tras la II Guerra Mundial, y de la que también son socios Canadá, Australia y Nueva Zelanda, es capaz de acceder a toda la información transmitida vía Internet, correo electrónico, fax y teléfono, empleándose mecanismos que tratan de neutralizar la encriptación. Su estructura es indiscriminada. Las comunicaciones interceptadas pasan el filtro de *Dictionary*, un programa que identifica palabras clave. Echelon usa más de 130 satélites y varios centros de recepción. ¡Se calcula que es capaz de filtrar diariamente más de 3 billones de comunicaciones!

virus (cada mes surgen ochocientos nuevos virus; a la fecha hay más de cuarenta y cinco mil). Varios de estos casos afectan de manera directa al derecho a la intimidad, que se ve agredido en multitud de ocasiones con suma facilidad, lo que prueba, en algunos supuestos, la inoperatividad de los medios de protección establecidos y que habían sido concebidos para una realidad muy distinta a la actual. Asimismo, el atentado del 11 de septiembre de 2001 en Estados Unidos ha sido la causa de la adopción de un conjunto de medidas por parte de varios Estados para mejorar su seguridad interior, algunas de las cuales frisan la inadmisibilidad desde una perspectiva garantista de la vida privada. En este sentido destaca la Combating Terrorism Act, aprobada el 13 de septiembre de 2001 por el Congreso estadounidense, que permite al FBI instalar, en los proveedores de acceso a Internet, sistemas que sirven para vigilar la circulación de los mensajes electrónicos durante 48 horas, sin necesidad de ninguna orden judicial (el propio 11 de septiembre, tan sólo algunas horas después de los atentados, agentes del FBI se presentaron en los locales de los proveedores de acceso a Internet AOL, *Earthlink* y *Hotmail*, para instalar en sus servidores el programa *Carnivore*).

Realmente la cuestión de la *seguridad* se ha convertido en central en todo lo que rodea a Internet. Aunque es evidente que no hay medios de comunicación totalmente seguros, en la Red los problemas de seguridad se agudizan a causa del elevadísimo número de usuarios y el diseño al que responde. El crecimiento y la complejidad hacen surgir elementos inseguros. La vulneración de la confidencialidad, de la integridad y de la disponibilidad del sistema son los objetivos de estos ataques (Vila Sobrino en Gómez Segade/Fernández-Albor/Tato, 2001, 59) con la finalidad, respectivamente, de leer la información transmitida, modificarla o colapsar una computadora de la Red para que no pueda desempeñar sus funciones. Las agresiones y peli-

gros no sólo provienen de piratas aislados sino también del propio sector público y del tejido empresarial.

La seguridad es una cuestión de la que dependerá la confianza de los usuarios, por lo que se relaciona de manera indisoluble al crecimiento de la Red. Ésta es una idea más que conocida y que recoge expresamente el Plan de Acción eEurope 2002 de la Comisión de la Unión Europea. También en el marco europeo, la directiva 2002/58/CE preceptúa que "el proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios" (artículo 4.1). Font (2000, 48) considera que los fundamentos de la seguridad son la autenticación, la integridad de la información, la privacidad, el no repudio, la datación y el acceso. A su vez, los elementos que influyen en la seguridad son muy variados, ya que van desde el tipo de instalación al tipo de aplicación, pasando por el carácter de la propia información que debe protegerse. La importancia de estas cuestiones es tal que se habla habitualmente de la necesidad de desarrollar una cultura de seguridad que permita adoptar nuevas formas de pensamiento y comportamiento cuando se usan los sistemas de información. Esta cultura de seguridad informática no puede olvidar en ningún momento los valores democráticos y la vigencia de los derechos fundamentales.

Las polémicas en el campo del *software* en torno al código abierto también tienen importantes connotaciones de seguridad. La apertura de *Microsoft* de parte del código fuente de su sistema operativo *Windows* a las agencias de seguridad de los gobiernos de sesenta países les permitirá a estas últimas desarrollar su propio programa de cifrado y, en colaboración con los técnicos de la empresa, crear diversas aplicaciones. De este modo, dicha empresa introduce la idea de código compartido para tratar de contrarrestar el auge de la cultura del código abierto, capitaneada por *Linux*.

Nuevas respuestas, por tanto, parece ser lo que hay que reclamar ante esta problemática, sin renunciar a las categorías existentes que pueden seguir siendo operativas con la calificación de principios. A lo que no puede renunciarse, como es obvio, es al núcleo básico de garantía de la vida privada que ofrecen los sistemas constitucionales. Por eso resulta acertada la posición de Pallaro (2000, 13) que defiende la validez integral para Internet de las reglas fundamentales del mundo *off-line*, porque lo fundamental es ese elemento esencial de garantía que no hay que desconocer pese a los cambios.

Según un informe del Parlamento Europeo conocido en febrero de 2000, la confidencialidad en Internet es mucho menor de lo que se pensaba ya que, entre otros datos, todos los correos electrónicos codificados por *Microsoft*, *Netscape* y *Lotus* pueden ser descifrados por un órgano de espionaje estadounidense llamado Agencia de Seguridad Nacional (cuyas siglas en inglés son NSA). Y no sólo eso sino que también el microprocesador de Intel *Pentium* III tiene un número de serie IPSN que permite identificar al sujeto que haga una transacción en Internet con él, a pesar de que Intel haya asegurado que el usuario puede impedir el acceso, mismo que con ciertas técnicas sigue siendo posible. Está claro que "la sociedad de masas permite el anonimato, pero la tecnología allana la vida privada" (Fernández Esteban, 1998, 142). Como señala Eugenio Díaz (1999, 150) "al abrir la ventana de nuestro ordenador a la calle de la red global de ordenadores entre sí conectados" se corre el riesgo de que

> nos expongamos (si no tomamos ciertas precauciones, y aún tomándolas) a la indiscreta observación de los demás usuarios de esa urdimbre de máquinas, programas e información digitalizada que, sin nuestro consentimiento y sin ni siquiera nuestro conocimiento, pueden ir anotando las huellas electrónicas personales que vamos dejando en nuestra ruta de internautas.

Los textos normativos no suelen definir la idea de intimidad, se limitan a recoger los casos que agreden a la misma y a reclamar la protección pertinente. La Declaración Universal de Derechos Humanos, en su artículo 12, establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación". Prosigue: "Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Parte de la doctrina distingue intimidad y privacidad (derivada directamente del inglés *privacy*) concibiendo ésta como más amplia que aquélla al aludir a datos no íntimos, pero que la persona quiere que no sean difundidos (aunque no hay que olvidar que no es ésta una cuestión pacífica entre los autores). La antigua ley española de protección de datos, la Ley Orgánica 5/1992, ya derogada, en su exposición de motivos, afirmaba que la intimidad "protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona" y "la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado". Incluso se llegan a establecer otros niveles diferentes (por ejemplo, en la doctrina alemana, aunque más bien con una finalidad pedagógica, se distingue entre *Intimsphäre*, *Privatsphäre* o *Geheimsphäre* y *Sozialsphäre*). Nosotros no vamos a entrar en esta distinción por considerar que la finalidad de este trabajo así lo aconseja. En el título hemos optado por hablar de intimidad por su mayor raigambre en el mundo jurídico hispano.

Además, hay que tener en cuenta que las diferencias culturales también son determinantes a la hora de establecer el ámbito normativo del derecho a la intimidad, al igual que lo eran para delimitar las libertades de comunicación. Es ésta distancia cultural, junto con la distinta rea-

lidad del desarrollo del mundo digital, la que percibe Kim Alexander y le lleva a afirmar que "los ciudadanos de Estados Unidos no disfrutan de la misma protección de la intimidad que los ciudadanos que viven en la Unión Europea", ya que la intimidad de los estadounidenses, en su opinión, cada vez está más "amenazada por las nuevas tecnologías, así como por el gobierno, de forma inadvertida o deliberada" (en Pau I Vall, 2002, 95). El relativismo cultural se acentúa todavía más y se hace patente con mayor evidencia en la Red.

Delimitar *a priori* la zona de intimidad de una persona no parece posible con total exactitud, ya que cada ser humano tiene necesidades diferentes relativas al espacio que quiere reservarse para sí. No obstante, sí hay ciertos elementos que comúnmente se consideran pertenecientes al susodicho espacio, como la vida sexual o las ideas y creencias. Una persona desea "no ser observada por cualquiera; después, si fuera observada y convertida en información notificable, difundible, que esa información sobre sí no sea difundida; y, más tarde, si acaso difundida la información que a ella se refiera, desea no ser personalmente, ni físicamente, ni patrimonialmente, ni moralmente invadida" (Eugenio Díaz, 1999, 152). La adecuada protección de la intimidad también es garantía de la libertad de expresión y del pluralismo que necesariamente deben existir en una sociedad democrática porque permite a la persona defenderse frente a las tendencias homogeneizadoras y represoras de lo no ortodoxo, gracias a lo cual el ciudadano tendrá mejor predisposición para comunicar sus opiniones.

Es común reconocer que la concretación del derecho a la intimidad y el punto de partida para su protección fue realizada por Samuel Warren y Louis Brandeis en su artículo "The Right to Privacy", publicado en 1890 en la *Harvard Law Review* (hay traducción en castellano de 1995 en la editorial madrileña Civitas), cuya gestación no deja de ser curiosa. En efecto, ante ciertos comentarios hechos en la prensa de Boston acerca del matrimonio de la hija del

senador Warren, éste encarga al abogado Brandeis (futuro integrante del Tribunal Supremo de los Estados Unidos) la elaboración del citado trabajo. Aquí se recoge ese intento de definición de la privacidad tantas veces repetido: el derecho a ser dejado a solas (*the right to be let alone*). La concepción unitaria del derecho que se desprende de este artículo fue más adelante contradicha, no sin polémica, por Willian Prosser en "Privacy", que vio la luz en el número 48 de la *California Law Review*, fechado en 1960. La evolución jurídica ha determinado que el derecho a la intimidad se convierta en un complejo de derechos: "es uno en su concepción y múltiple en cuanto a sus contenidos" (Ruiz Miguel, 1995a, 76). Fernández Segado (1997, 9) afirma que este derecho "ha asumido una nueva dimensión por virtud de la cual ya no se entiende tan sólo en un sentido puramente negativo, de rechazo de la información de extraños en la vida privada...; bien al contrario ha pasado a tener un contenido positivo".

Sin duda, la complejidad de la realidad actual exige una aproximación a la intimidad que tenga en cuenta los diversos aspectos que contempla, entre los cuales se halla el derecho a controlar la información acerca de uno mismo, lo que tiene una insoslayable conexión con los temas informáticos, que es a lo que nos referimos en el epígrafe siguiente. Es innegable que Internet afecta las expectativas razonables de privacidad de una persona. Este enriquecimiento del contenido y de la naturaleza jurídica del derecho a la intimidad ha dado lugar a la aparición de una dimensión institucional democrática del mismo, subrayada por Schmitt Glaeser, que va más allá de su mera consideración como derecho de defensa. Esta dimensión posibilita el desarrollo de la identidad personal y, por ende, de la actividad social que configura la comunidad y que caracteriza a una democracia viva (Schmitt Glaeser, 1989, 43). Así, como asevera Ruiz Miguel (1995b, 3219), el derecho a la intimidad es una garantía objetiva del pluralismo y de la democracia, por lo que "para que una democracia esté

viva, es preciso que respete la intimidad de quienes la componen, pues sólo así, desde la libertad e independencia de cada ciudadano puede construirse una sociedad libre".

II. Intimidad e informática

1. *Las exigencias de la intimidad*

Suele ser habitual en los textos constitucionales la previsión del derecho a la intimidad (en este sentido se pueden citar el artículo 22 de la Constitución belga, el 8o. de la Constitución finlandesa, el 9o. de la Constitución griega o el 26 de la Constitución portuguesa). En cambio, es menos habitual en derecho comparado la existencia de previsiones específicas para las cuestiones ligadas a la informática. En México las garantías de la intimidad hay que deducirlas, a falta de previsión constitucional expresa, de la libertad religiosa y de la inviolabilidad del domicilio.

Parece que fue Francia el primer Estado donde se dicta una legislación específica de protección frente a la informática a través de la Ley 78/17, del 6 de enero de 1978, sobre Informática y libertades, que hoy en día resulta aplicable a Internet. No obstante, usaremos como ejemplo, para ilustrar las ideas que queremos exponer, la vigente Constitución española de 1978, donde se conecta la intimidad y la informática. Dicho texto recoge en su artículo 18, entre otras ideas, el derecho a la intimidad, la inviolabilidad del domicilio, el secreto de las comunicaciones, y establece, en el apartado 4, un encargo al legislador consistente en la limitación por ley del "uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". La redacción de este último apartado se efectuó con base en la idea de que la generalización de la informática iba a originar crecientes problemas que reclamaban la adopción de medidas específicas para enfrentarlos.

La regulación constitucional española ha sido objeto de diversas críticas, como las de Pérez Luño (1999, 338 y ss.), que entiende que se parte de "un planteamiento fragmentario e individualista de la compleja serie de cuestiones de matiz personal y social que hoy se debaten y suscitan", problema que no se resuelve con el complemento del artículo 105 b) de la Constitución, antes bien genera un "defecto sistemático".

El límite que impone la ley al uso de la informática se ha interpretado no sólo como la constitucionalización de la "defensa de todos y cada uno de los derechos de los ciudadanos frente al uso indiscriminado de los medios informáticos" (Álvarez-Cienfuegos, 1999, 15), sino también como el reconocimiento de un nuevo derecho fundamental que va más allá de un mero mecanismo de garantía al verse desbordada la intimidad por el bien jurídico a proteger en este último caso (la genérica defensa de la personalidad).

Podemos traer a colación la interpretación que se desprende de la sentencia del Tribunal Constitucional español 254/1993, fundamento jurídico 6o., reiterada en otras sentencias:

> Nuestra Constitución (la española) ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona... Estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".

Este nuevo derecho suele ser denominado por la doctrina "derecho a la autodeterminación informativa" (Lucas Murillo de la Cueva, 1990, pp. 27 y ss.), considerado "un

derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona" (sentencia del Tribunal Constitucional español 11/1998, del 13 de enero). No obstante, parte de la literatura se muestra discrepante con tales posiciones y entiende que estamos ante meras concretaciones del derecho a la intimidad o al respeto de la vida privada en el campo de las nuevas tecnologías de la información. Es el caso de Ruiz Miguel que aduce la naturaleza compleja del derecho a la intimidad (no reducible a las categorías de un "derecho de defensa"), los elementos subjetivos o sistemáticos de la definición de lo íntimo o privado (más allá de los criterios objetivo-sustantivos) y diversas sentencias del Tribunal Europeo de Derechos Humanos y del propio Tribunal Constitucional español (Ruiz Miguel en Gómez Segade/Fernández-Albor/Tato, 2001, 399). En esta tesitura, el citado autor entiende de utilidad la distinción entre principio y reglas, considerando la intimidad como un principio que se concretaría en diversas reglas, una de las cuales sería la intimidad informática (*ibidem*, 400). Jurisprudencia constitucional española más reciente mantiene una posición intermedia al reconocer un derecho con sustantividad propia ("el derecho a la protección de datos personales") y, al mismo tiempo, considerar que se conecta con el derecho a la intimidad (sentencias 290/2000 y 292/2000).

Sea como fuere, y al margen de esta polémica, la relevancia de las cuestiones informáticas en este punto se suele redirigir, tanto en el campo normativo como en el doctrinal, a la problemática de la protección de datos, sobre la que volveremos en el último apartado de este capítulo, si bien es evidente que semejante visión es bastante parcial y simplista en comparación con el conjunto de aspectos que surgen; es decir, que la problemática de la protección de datos es una de las varias que nacen de la interacción entre informática e intimidad y, por tanto, no agota, ni mucho menos, la misma.

La preocupación por estas cuestiones es compartida en otros muchos instrumentos normativos de ámbitos y latitudes muy diferentes. Así, en el continente europeo, y también de conformidad con la protección de datos, hay que nombrar el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; la directiva 95/46/CE, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de esos Datos (basada en el citado Convenio 108 del Consejo de Europa); la 97/66/CE, sobre el Tratamiento de Datos Personales y la Protección de la Intimidad en el Sector de las Telecomunicaciones; la 2002/58/CE, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas (que sustituiría a la anterior al derogarla el 31 de octubre de 2003). La directiva 95/46 crea, en el artículo 29, un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro de la Unión Europea, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Para el estudio de la aplicación de las dos primeras directivas citadas este grupo, llamado Grupo del Artículo 29, creó, a su vez, un grupo de trabajo llamado *Task Force Internet*, que trata de fomentar los productos útiles para proteger la privacidad. En sus reflexiones se aboga porque las directivas citadas se apliquen también a Internet, se anima a que las empresas de *software* y de *hardware* elaboren productos que protejan la intimidad y se pretende establecer pautas que se deberían seguir de forma escrupulosa en la interceptación legal de las telecomunicaciones. También podemos citar la decisión 276/1999/CE, que aprueba un plan plurianual de acción comunitaria para propiciar una

mayor seguridad en la utilización de Internet. Como se ve, la Unión Europea se esfuerza por mantener la actualidad de las cuestiones relativas a la protección de datos de la intimidad. La sustitución de la directiva 97/66/CE por la 2002/58/CE obedece a tal idea como expresamente lo recoge el considerando 4 de esta última.

La Comisión Especial sobre Redes Informáticas creada en el Senado español el 14 de marzo de 1998 (y cuyo Informe fue aprobado por el pleno del Senado el 17 de diciembre de 1999), en la cuarta de sus conclusiones, afirma que "el ordenador personal y el domicilio electrónico son inviolables". Prosigue: "Ninguna entrada o registro podrá hacerse sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. Se garantizará el secreto de las comunicaciones electrónicas y la privacidad de los datos". Se están parafraseando los párrafos segundo y tercero del artículo 18 de la Constitución española para equiparar al domicilio señalado en este último artículo el domicilio electrónico y la computadora personal, y para incluir en las comunicaciones las de tipo electrónico. Esta última idea ya estaba clara pues la redacción del artículo 18.3 de dicha Constitución da pie a interpretar la noción de comunicación de modo amplio, más allá de las tres formas a las que alude expresamente (postales, telegráficas y telefónicas), alusión que es, en todo caso, ejemplificativa. Si partimos de la idea de intimidad se recogen, por tanto, el derecho a la autodeterminación informativa y una lectura en esta clave de la inviolabilidad del domicilio y del secreto de las comunicaciones.

El derecho a la intimidad que, junto a una dimensión relacional útil para la existencia colectiva, protege una zona espiritual íntima, o sea, un reducto personal y privado frente a posibles agresiones exteriores y frente al conocimiento de los demás, tiene particulares exigencias cuando se enfrentan la informática y las redes, llegando incluso a propiciar, según se indicó más arriba, la configuración de un nuevo derecho fundamental, aunque de

existencia discutida. Ese ámbito propio y reservado resulta "necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (sentencia del Tribunal Constitucional español 231/1988, fundamento jurídico 3o.). Como señala Pérez Luño (1999, 317), el respeto a la intimidad se ha convertido en "una de las exigencias más acuciantes que hoy gravita sobre la sociedad tecnológicamente avanzada". Más adelante este autor reitera la misma idea al indicar que la "amenaza latente para el ejercicio de las libertades, que obedece a las condiciones en las que se desarrolla la vida colectiva de nuestra época caracterizada por la revolución tecnológica, se ha hecho particularmente acuciante en relación con el derecho a la intimidad" (*ibidem*, 345-346).

Esta defensa de la intimidad no sólo debe ser vista desde una postura negativa, como posibilidad de reaccionar frente a una invasión, sino también desde una dimensión positiva que permita al sujeto controlar las informaciones que le afecten ("un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona" —Sentencia del Tribunal Constitucional español 44/1999, fundamento jurídico 2o.— o "poder de control y disposición sobre" los datos personales —Sentencia del Tribunal Constitucional español 290/2000, del 30 de noviembre—). Por un lado, entre otros aspectos, lleva a que no se utilicen los datos personales para fines no consentidos por la persona a la que hacen referencia tales datos y a que se puedan controlar dichos datos cuando se hallan en un programa informático (*habeas data*). Este control "sobre la publicidad de la información relativa a nuestra persona y familia" (de nuevo una sentencia del Tribunal Constitucional español, la 144/1999, del 22 de julio) supone derecho de información, de acceso, de rectificación y cancelación. Por otro lado, la defensa de la intimidad garantiza la no entrada en el propio ordenador personal sin consentimiento del titular. A su vez, el correo electrónico se conecta de modo directo con el derecho al secreto de las

comunicaciones, que hay que interpretar, como acabamos de señalar, de un modo amplio e incluir en su ámbito nuevos tipos de comunicación como es el ahora aludido.

La intimidad, en suma, "garantiza al individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros, sean éstos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida" (sentencia del Tribunal Constitucional español 134/1999, del 15 de julio).

Pese al tono genérico que estamos usando en este apartado, es cierto que las diferencias entre ordenamientos jurídicos matizan muchas de las cuestiones expuestas. Así, la concepción europea continental de los derechos fundamentales es más amplia que la anglosajona en el sentido de que los hace oponibles también frente a los particulares y no sólo frente a los poderes públicos, mientras que la concepción anglosajona gravita sobre la aplicación frente a los poderes públicos. Esto tiene consecuencias en el tema que nos ocupa y explica, por ejemplo, cómo en Estados Unidos la protección de la intimidad se remite a códigos de conducta adoptados por los agentes privados, mientras que la Privacy Act de 1974 carece en determinados supuestos de verdaderos mecanismos coactivos públicos de imposición.

2. *Nuevas formas de agresión*

Los avances técnicos han dado lugar a nuevas formas de agresión a la intimidad y a la vida privada, en un elenco que no está, ni mucho menos, cerrado y con una escala de gravedad diversa. Así, podemos citar:

- La entrada en el disco duro de un ordenador sin consentimiento.
- La elaboración de perfiles del navegante (construidos en torno a su vida privada) con fines publicitarios u otros más graves.

- La simple acumulación o registro de datos sin consentimiento.
- La transferencia de datos sin consentimiento.
- El empleo de una dirección IP asignada a otro ordenador.
- La interceptación de mensajes de correo electrónico y de las comunicaciones en general (leyendo y/o modificando su contenido).
- La suplantación de personalidad de un usuario o de la identidad de una computadora.
- El hostigamiento electrónico.
- El uso indebido de directorios de correo electrónico o listas de usuarios.
- Alteración o destrucción de información.
- Impedimento para acceder a la información (interrupción del servicio).
- El acceso a la cuenta del administrador.

Los perfiles de esas agresiones resultan en algún caso confusos, superponiéndose y conectándose. A veces, como veremos, el *software* que se emplea en tales actividades se crea de forma específica para ello. Estas agresiones, algunas de ellas fáciles de realizar, son potencialmente muy graves por la mundialización a la que pueden llegar. Si un aspecto de la vida privada de una persona es conocido por un pirata informático y lo mete en la Red, en potencia una enorme cantidad de sujetos puede acceder a él desde cualquier parte del planeta habida cuenta las características y el desarrollo actual de Internet. Es lo que indica Schachter (2002, 390), cuando señala que algo dicho o hecho por un ciudadano "puede ser diseminado por todo el mundo de manera instantánea", permaneciendo "accesible para ser recuperado virtualmente de modo indefinido". El anonimato que es posible buscar en Internet, al que coadyuvan las dimensiones de la Red y las dosis de anarquía que en ella existen, favorece que se produzcan vulneraciones de los derechos que conciernen a la vida privada dado que el

agresor se siente más seguro, aunque esto no puede llevarnos a posiciones extremas que traten de prohibir el anonimato en los intercambios, como la de Cebrián (1998, 103). De igual forma, la auto organización y el caos de la Red facilitan su vulnerabilidad. Por tanto, muchos son los factores que complican tales agresiones. Se ha intentado retratar esta situación con afirmaciones que reflejan la peligrosidad de la misma, como la del vicepresidente de *Microsoft*, Nathan Myrhvold, que indica que en la Red no existen ni identidad, ni vida privada, ni propiedad.

Pero así como el mundo digital ha posibilitado estas nuevas agresiones, su tecnología también permite articular mecanismos de defensa, mecanismos impensables desde la tecnología analógica. No obstante, no cabe duda de que el desarrollo tecnológico hace que "cada día sea más difícil conservar intacto el ámbito de la propia vida privada" (Fernández Esteban, 1998, 137). Es, en parte, el precio por el avance digital.

El mundo de Internet, incluso, ha creado una *jerga* particular, parte de la cual tiene que ver con las vulneraciones que se producen del derecho a la intimidad. De este modo, un "agujero de seguridad" es un aspecto de *hardware* o de *software* que hace vulnerable al equipo informático ante los ataques. Además, se habla en castellano de "pirata informático", o en inglés de *hacker* (sujeto que se dedica a traspasar las barreras de seguridad de los equipos informáticos buscando errores o malas configuraciones sin ánimo de perjudicar), de *cracker* (sería la versión malvada del anterior al actuar con el fin de causar un perjuicio intentando acceder a una computadora o a una red sin tener autorización para ello) y de *phone phreaker* (pirata especializado en compañías telefónicas). También tenemos al *virucker*, sujeto que introduce virus en equipos informáticos ajenos. Los tribunales españoles, como los de otros países, ya han tenido que enfrentarse a algún caso sobre acceso ilegal a un sistema informático. El primero parece haber sido el de *hispahack*, en donde se definió el fenó-

meno *hacking* como una intrusión informática o interferencia o acceso no autorizado a un sistema informático. Frente a estas intenciones de acceso, por seguir con lo de la jerga, se interponen "cortafuegos" (*firewalls*), que son programas de seguridad que protegen los ficheros de ciertos servidores para impedir la incursión de personas no autorizadas; "sacos de arena" (*sandbox*), con el objeto de establecer un área segura no conectada a la red; y "antivirus", para escanear los discos y comprobar la existencia de virus, eliminándolos si resulta posible.

Los programas que se usan para *atacar* a los equipos informáticos forman parte de los denominados "códigos maliciosos" o "*software* malintencionado", un conjunto de programas que producen resultados no deseados. En este orden de cosas tenemos, en primer lugar, a los "troyanos" (o "caballos de Troya" —*trojan horses*—). Se trata de instrucciones introducidas en la secuencia de otros programas legales que realizan funciones no autorizadas, destruyendo ficheros o capturando información mientras parecen ejecutar funciones correctas. El "troyano" es instalado por el propio equipo que sufre el ataque pensando que hace algo no perjudicial cuando, en realidad, además de hacer, a lo mejor, eso, hace otra cosa clandestinamente (averiguar contraseñas, borra información, crea nuevos usuarios, envía un correo, etcétera). Los "troyanos" están camuflados en programas que son inofensivos. En segundo lugar nos encontramos con los "gusanos" (*worms*), que son programas que tras introducirse en un sistema son capaces de reproducirse por sí solos con el objetivo de realizar sabotajes. El gusano no necesita de otro programa para funcionar. Se va duplicando y ocupando memoria hasta que su tamaño impide realizar al sistema correctamente su trabajo. Los "gusanos" pueden alojarse en los "troyanos". Asimismo, también hay que citar, en tercer lugar, a los virus, que son programas que se cuelan en las computadoras y tienen capacidad de replicarse, aunque no actúan, como los "gusanos", de forma autónoma, sino que el

usuario tiene que efectuar alguna acción para que se propague, como, por ejemplo, ejecutar un archivo. Los virus también se pueden esconder en un "troyano". Se trata de programas capaces de reproducirse que modifican otros programas o alteran ficheros. Virus famosos por el impacto que han tenido y los daños causados son, por ejemplo, el Sircam, el Código Rojo o el Nimda. De igual modo, en cuarto lugar, se pueden traer a colación las "bombas de relojería" o "bombas lógicas" (*logic bombs*), que son parecidas a los "troyanos" y que actúan en un momento predeterminado buscando causar el mayor daño gracias al "temporizador" que contienen. De esta forma, se activan en determinadas condiciones, como en una fecha o ante la presencia o ausencia de un dato en un fichero. Por lo general, su efecto es liberar un virus o un "troyano". A su vez, en quinto lugar, un "rastreador" o "analizador de red" (*sniffer*) es un programa rastreador capaz de leer toda la información que circula por una red de computadoras en busca de usuarios, contraseñas u otros datos que vuelcan en un fichero. En sexto y último lugar vamos a citar los *remailers* y las *electronic mail bombs*, programas relacionados con el correo electrónico que originan órdenes de envío de correo desde un origen a diversos destinatarios o a uno solo. Hay que tener en cuenta que, por lo general, los programas que atacan a la intimidad de un usuario suelen reunir características de varios de los tipos básicos acabados de ver.

Igualmente, para realizar agresiones a la intimidad se usan otros mecanismos que no son "códigos maliciosos". Es el caso de la "galleta" o "chivato" (*cookie*). En este caso estamos ante dispositivos que se colocan dentro de las computadoras y que recaban datos de la misma y de su usuario sin que éste detecte que está siendo inspeccionado. Una *cookie* es un fichero, no un programa, que llega al equipo informático al consultar una página *web* y que en principio no tiene malas intenciones sino que busca ser cooperativa al facilitar la navegación, aunque el uso que a veces se hace de ellas resulta, como indicaremos más

abajo, inadmisible al convertirse en una vía de acceso para realizar los ataques. Una de sus utilidades es la de personalizar las páginas más visitadas, lo que permite al usuario acceder a la sección que le interesa descartando otras, o que se cargue la página en el idioma elegido inicialmente, o que la carga sea más rápida en la sección que presenta mayor interés. La identificación del usuario también facilita operaciones de comercio electrónico, como la oferta directa de productos que le interesan con asiduidad o recoger artículos en un "carrito de compra" mientras se realiza la visita. Esta utilidad es reconocida por la directiva 2002/58/CE para, por ejemplo, "analizar la efectividad del diseño y de la publicidad de un sitio *web* y para verificar la identidad de usuarios partícipes en una transacción en línea" (considerando 25). Este fichero que supone la *cookie* contiene un conjunto de datos que un servidor *web* envía al equipo informático desde el que se está navegando, datos relativos a la utilización que se ha hecho de las páginas de dicho servidor (dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etcétera). Esta información, que se almacena en un fichero en el directorio del navegador, se utiliza en una próxima visita al mismo servidor. Las *cookies* tienen fecha de caducidad, a partir de la cual dejan de ser operativas. En *Explorer* dichas *cookies* se almacenan en el disco duro del usuario, en la carpeta "C:\Windows\Cookies" sobre archivos de texto (extensión TXT) como si fueran ficheros con nombres del estilo "nombre de *usuario@servidor*". En *Netscape* se ubican en el archivo de texto "Cookies.txt" en "C:\Archivos de programa\Netscape\Users\Nombre de usuario".

Las formas de ataque pueden ser divididas en cuatro grandes categorías: interrupción (se evita que se transmita información), interceptación, modificación y fabricación (el atacante introduce elementos nuevos) (Font, 2000, 27-28). Frente a ellas, al margen de las defensas legales, se pueden establecer medios de protección en la propia compu-

tadora (como "cortafuegos" o *firewalls* individuales) o desde la red (como otros tipos de "cortafuegos", claves de acceso, recurso a técnicas criptográficas o programas que bloquean la entrada de virus). Estas defensas pueden responder a la lógica de una seguridad activa, si se articulan como medidas de prevención, o de seguridad pasiva, si se configuran como medidas de corrección. De igual modo, el usuario puede proteger su intimidad acudiendo a otras soluciones, como el protocolo P3P (*platform for privacy preferences*, un análisis del mismo puede verse en Enzmann, 2000), desarrollado por el consorcio *www* con el objeto de facilitar los intercambios y la negociación entre un navegante y un sitio *web*. Se trata de un sistema estandarizado de preguntas entre el sitio y el *software* del usuario que permiten conocer la política de ese sitio sobre la información personal de los usuarios. Si las prácticas del sitio coinciden con las preferencias del usuario la negociación continuará. En caso contrario, el usuario será avisado para que tome la decisión de continuar o no.

III. El correo electrónico

El correo electrónico es uno de los más destacados avances de la era de la sociedad de la información que ha originado algunas de las nuevas formas de agresión a la intimidad que hemos citado. Un fenómeno tan antiguo como la propia especie humana, el de la comunicación, se lleva a cabo a través de un soporte desconocido hasta hace muy poco: el mensaje se digitaliza para enviarse al destinatario a velocidad luz por la Red. De esta forma, se conectan dos equipos informáticos a través de un servidor. El correo electrónico origina necesidades de tratamiento jurídico igualmente novedosas, que poco a poco habrá que ir construyendo y sedimentando. Pero también exige que se tengan en cuenta una serie de cuestiones ya presentes en otros fenómenos comunicativos. En este sentido, hay que subrayar la cobertura que le da el derecho al secreto de

las comunicaciones, lo que nos parece innegable a pesar de que haya habido algunas voces discrepantes. Los textos constitucionales suelen recoger este derecho (artículos 10 y 18 de la Ley Fundamental de Bonn, 29 de la Constitución belga, 72 de la Constitución danesa, 18.3 de la Constitución española, 15 de la Constitución italiana, o 34 de la Constitución portuguesa, entre otros).

El derecho al secreto de las comunicaciones se concibe habitualmente como una proyección de la intimidad y privacidad del individuo, además del papel que también juega en otros campos, como el de la defensa de la libertad de expresión, aunque bien es cierto que se puede sostener una concepción que desligue al secreto de las comunicaciones de la intimidad, concepción preferida por nosotros, ya que la comunicación se protege por si misma con independencia de si su contenido afecta a la esfera privada del individuo o no. Al margen de la postura que se adopte en esa cuestión, detrás de este derecho hay una fundamentación y una finalidad que no varían en función del soporte que se emplee para realizar el proceso comunicativo siempre que éste tenga lugar a través de un canal cerrado. El ejemplo que nos da la Constitución española es ilustrativo al respecto: su artículo 18.3 protege la comunicación frente a cualquier interceptación llevada a cabo por terceros ajenos (sentencia del Tribunal Constitucional español 114/1984, fundamento jurídico 7o.), y la protege desde un punto de vista formal, es decir, independientemente de su contenido (sentencias del mismo órgano 114/1984, fundamento jurídico 7o.; 34/1996, fundamento jurídico 4o.; 127/1996, fundamento jurídico 4o.), si se hace tan sólo una enumeración de soportes a título ejemplificativo, por lo que hay que interpretar que la comunicación se protege con independencia del soporte. En el contexto en el que nos movemos el medio técnico usado para llevar a cabo la comunicación tiene que perder importancia para dársela a la efectiva realización de una comunicación de un medio no abierto, que habrá que reputar como secreta. Un correo

electrónico no es como una postal, que es un canal abierto en el que no hay expectativa de secreto, sino que es un canal cerrado: el mensaje se envía a un destinatario que posee una dirección determinada que atestigua que es con él con quien se quiere establecer la comunicación y no con otra persona.

Los mensajes de correo electrónico antes de alcanzar su destino circulan por la Red usando una serie de soportes técnicos y servidores, que en su mayor parte son privados. Son una especie de textos abiertos que en cualquier etapa intermedia de su distribución pueden ser leídos y detectados su remitente y destinatario. Es importante, por ello, que los proveedores de servicios se comprometan a mantener la confidencialidad, ya que tienen capacidad técnica para abrir y leer los mensajes, tanto los enviados como los recibidos. La propia Ley española 11/1998, del 24 de abril, General de Telecomunicaciones, impone el deber de secreto de las comunicaciones a "los operadores que presten servicios de telecomunicaciones al público o exploten redes de telecomunicaciones accesibles al público" (artículo 49). Está claro que la mayor o menor facilidad técnica del que gestiona el correo para leerlo no puede tener ninguna traducción jurídica salvo la de exigirle el mantenimiento del secreto. También es evidente que a los terceros que no sean proveedores de servicio les son de aplicación las obligaciones derivadas del derecho al secreto de las comunicaciones. Sus actos de injerencia serán ilícitos.

A la complejidad jurídica de las cuestiones ligadas, en general, al mundo digital y, en particular, al correo electrónico, hay que sumar, desafortunadamente, un tratamiento en la práctica que en diversas ocasiones no es el más adecuado para la intimidad ni para el secreto de las comunicaciones. El principio interpretativo *favor libertatis*, que lleva a escoger las soluciones que mejor maximicen los derechos fundamentales, parece por momentos obviado. El tratamiento judicial que recibe esta problemática aún ofrece en diversos países muchas dudas y, aunque todavía

está en sus primeros momentos, la impresión no es del todo satisfactoria. Supongo que la atención pública respecto a este tipo de fenómenos irá creciendo y que los conflictos jurídicos en torno al correo electrónico se multiplicarán.

En el ámbito laboral ya tenemos casos que han trascendido de manera importante a la opinión pública y a los medios de comunicación, como, por citar ahora sólo un ejemplo referido a España, los despidos disciplinarios por mal uso del correo electrónico en una conocida entidad bancaria y que fueron analizados por el Tribunal Superior de Justicia de Cataluña en su sentencia del 14 de noviembre de 2000. En ella se afirma que la utilización por parte del trabajador de "los medios informáticos con que cuenta la empresa, en gran número de ocasiones, para fines ajenos a los laborales" hacen procedente la reacción empresarial consistente en el despido disciplinario. El razonamiento llama, cuando menos, la atención dado que el tiempo de trabajo perdido efectivamente fue muy pequeño, por lo que el principio de proporcionalidad se resiente. No obstante, no entra de lleno en la problemática de la intervención del correo electrónico de un trabajador. Por otra parte, todavía parece que no hay líneas jurisprudenciales claras en este sentido, aunque necesariamente, antes o después, se tendrá que entrar de lleno en semejante tema. El derecho comparado nos ofrece soluciones legislativas distintas. De este modo, por ejemplo, en Gran Bretaña no se reconoce la inviolabilidad del correo electrónico de los trabajadores, a diferencia de la normativa alemana y francesa, más proteccionista en este sentido. La denominada Fundación para la Intimidad, con sede en San Francisco (www.privacyfoundation.org), reflejaba en un informe de 2001 que 27 millones de trabajadores de todo el mundo que utilizan Internet son vigilados por sus jefes, que supervisan el uso que dan al correo electrónico de la empresa con el objeto de acumular información que pueda servir, en el futuro, para justificar despidos u otras medidas disciplinarias.

Es sabido que el contrato de trabajo conlleva una facultad de control referida al cumplimiento de la obligación contratada. Puede afirmarse, en general y sin entrar en particularismos nacionales, que las facultades de ejercer el control por parte de la empresa se han interpretado de una manera amplia, a pesar de que es cierto que el correo electrónico en una empresa es una herramienta corporativa y el empresario ha de ejercer cierto control para evitar responsabilidades derivadas del uso del mismo. El empleador escoge el medio de control más apto para el logro de la finalidad perseguida. La facilidad con que los medios de comunicación de la empresa pueden ser objeto de un uso no acorde con el fin para el que se han establecido lleva a que se admitan sin apenas dificultad medidas de control con el propósito de comprobar tales extremos.

Pero un aspecto es que se analicen los destinatarios de los correos electrónicos que envía un trabajador desde el puesto de trabajo y con los equipos del empleador para determinar el grado de relación de dichos correos con las labores de la empresa, y otra muy distinta es proceder a la apertura de tales correos para averiguar su contenido en concreto. Esto último parece desproporcionado para el fin perseguido y, por tanto, contrario al principio de mínima intervención en las actuaciones restrictivas de derechos fundamentales. En esta línea de búsqueda de proporcionalidad la Commission Nationale Informatique et Libertés francesa (CNIL) entiende que el empresario no puede registrar las conversaciones telefónicas ni la integridad de los números de teléfono marcados por sus empleados, lo que podría aplicarse al ámbito de la Red para entender que en el análisis de algunas direcciones de destino de los correos de los trabajadores sólo es relevante aquella parte de la misma que sirva para conocer si estamos ante un correo electrónico motivado en razones de trabajo o personales. Afirmar el carácter limitado del derecho a la intimidad o del derecho al secreto de las comunicaciones, que tienen que recibir un tratamiento que los haga compatibles con

otros derechos e intereses legítimos (lo que permitirá una adecuada disciplina del negocio jurídico en el que nos hallemos), no debe permitir pasar a un importante desconocimiento de los mismos en una suerte de salto cualitativo de dudoso respeto con los principios constitucionales. Se trataría de una huida hacia delante en favor de los intereses del empleador sin preocuparse de las exigencias constitucionales y de la autorización judicial que debe mediar para legitimar una intervención de comunicaciones.

Además, si se quiere ir más lejos, no hay que desconocer que los destinatarios también son un elemento englobado por el secreto de las comunicaciones y por la propia intimidad del sujeto que envía el mensaje; en este sentido, hasta cierto punto resulta irrelevante la titularidad de los medios empleados para la transmisión. La propiedad del equipo informático usado para enviar el mensaje no es clave, en modo alguno. En todo caso, la intervención de las comunicaciones del trabajador tiene que centrarse en lo relevante para la finalidad empresarial del control (ver si son de naturaleza comercial o no —para lo cual puede ser más que suficiente conocer el destinatario—), debe ser un recurso que dure el tiempo estrictamente necesario para lograr el fin perseguido y, además, tiene que ser el último recurso, por lo que es necesario acudir antes a otros medios de fiscalización. Otra cuestión es que medie consentimiento del trabajador, aunque en este punto a veces se alegan consentimientos que se reputan implícitos de una manera harto discutible. ¿El hecho de que el trabajador conozca la política empresarial de control de comunicaciones supone su autorización para proceder a la revelación de su contenido? Creemos que no, máxime cuando por lo general el control resulta en la práctica circunstancial y aleatoria.

En definitiva, el correo electrónico entra en el radio de acción del derecho al secreto de las comunicaciones y exige una atención mayor que la vía postal clásica dada la presencia, para algunos, de sombras e incertidumbres al

respecto, que nosotros no vemos. Los poderes públicos tienen que velar por la garantía del secreto de las comunicaciones electrónicas. En este sentido, la directiva 2002/58/CE afirma que "los Estados miembros (de la Unión Europea) garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público" (artículo 5.1, en sentido similar que el considerando 21).

IV. Criptografía frente a interceptación

1. *La criptografía como posibilidad*

Como defensa frente a los peligros que suponen para la intimidad las redes informáticas muchas veces se aboga por la encriptación, que es un proceso de protección de datos mediante un cifrado de los mismos que evita una manipulación no deseada. De un texto claro (*plaintext*) se pasa a un criptograma (*ciphertext*). Los beneficios de la misma han llevado a considerarla como "panacea casi universal" (Bertrand/Piette-Coudol, 2000, 93). Hoy por hoy, la encriptación es el remedio por excelencia frente a las agresiones a la intimidad consistentes en la interceptación de los mensajes y datos enviados a través de la Red, aunque no sirve como respuesta frente a otros tipos de agresión. La seguridad del correo electrónico, por ejemplo, aumenta de manera importantísima aplicando sistemas criptográficos. Estos métodos aportan confidencialidad (al evitar la interceptación o, mejor dicho, al hacer inútil el esfuerzo del pirata informático puesto que no comprende lo que intercepta), autenticidad (con el certificado digital) y fiabilidad para el contenido del mensaje (a través de la firma electrónica avanzada y la integridad que garantiza). Como se ve, tales métodos tienen finalidades antitéticas, es de-

cir, y como recuerda Lessig (2001, 97), "la misma tecnología posibilita tanto la confidencialidad como la identificación".

La Unión Europea reconoce la utilidad de las técnicas criptográficas en virtud de que su Comisión adoptó el 8 de octubre de 1997 una comunicación dirigida al Parlamento Europeo y al Consejo sobre "El fomento de la seguridad y la confianza en la comunicación electrónica. Hacia un marco europeo para la firma digital y el cifrado". La encriptación se encuentra expresamente admitida, por su parte, en el artículo 52 de la Ley General de Telecomunicaciones española de 1998.

2. *Técnicas de cifrado*

La criptografía emplea algoritmos (ecuaciones matemáticas que contienen una variable) y claves (variable numérica utilizada en combinación con un algoritmo). Las técnicas clásicas de cifrado de datos utilizaban una única clave secreta, generalmente construida restando una cantidad a los números que representan a las letras o sustituyendo cada letra por la situada "x" posiciones más adelante. El emisor aplicaba esta clave para cifrar el mensaje, que a continuación era enviado al receptor, el cual también debía conocer dicha clave para proceder a su decodificación. Este sistema tenía la ventaja de la rapidez y la simpleza que suponía tener una única clave. En cambio, y como elemento negativo, era necesario un canal de transmisión realmente seguro puesto que una vez interceptado el mensaje no resultaba demasiado complicado descifrarlo. Esta técnica se denomina encriptación simétrica o de clave privada y su origen se encuentra muchos siglos atrás, aunque bien es cierto que los algoritmos que se utilizan ahora, basados en particiones, reorganizaciones y fusiones (como el DES —*data encrytpion standard*—) poco tienen que ver con los desplazamientos en el alfabeto mencionados.

En la actualidad se usa el llamado sistema de encriptación asimétrica o de clave pública, creado en 1976 por Diffie y Hellman, si bien el algoritmo de este tipo más utilizado hoy en día es el denominado RSA, siglas que tratan de honrar a sus creadores, Rivest, Shamir y Adleman. En la criptografía asimétrica existen dos claves, una pública y otra privada, que sirven tanto para codificar como para decodificar, pero no por sí solas sino que son necesarias las dos. En efecto, si una codifica el mensaje la otra es imprescindible para decodificarlo. La complementariedad de ambas se basa en una fórmula compleja que hace extremadamente difícil que del conocimiento de la clave pública se llegue a la clave privada. La relación matemática entre las claves se realiza a través de una función *hash*. En la práctica, la que se emplea para codificar es la clave pública, que es la que se conoce porque el que la posee (el destinatario) la remite a quien va a enviar información, y la que se utiliza para decodificar es la clave privada, que es la que permanece oculta. Las dos obran en poder de un mismo sujeto, que será el destinatario de una comunicación. Si alguien quiere enviarle algo cifrado a ese sujeto le solicita que le comunique su clave pública. Tras ello, el remitente codificará el mensaje con la clave pública del receptor. Éste, una vez que le llegue dicho mensaje, utilizará su clave privada para decodificarlo. De esta forma, no es necesario que la clave privada salga del dominio del sujeto en cuestión, con lo que el riesgo de ser robada es mucho menor que el que existe en el antiguo sistema de única clave secreta, clave que forzosamente había de transmitirse por un conducto u otro al receptor para que procediera al descifrado. Así, el sistema de la doble clave no necesita un canal seguro para enviar la información pues si se intercepta, el descifrado resulta extremadamente difícil, llegando a supuestos en los que, en la práctica, es totalmente desaconsejable dado el tiempo que llevaría. El punto de partida hoy recomendado para elaborar las claves son productos de más de cien dígitos, con lo que se originan tales

problemas de factorización que hacen inviable el proceso de descubrimiento de las claves, incluso para la todopoderosa National Security Agency (NSA) estadounidense. Cuanto mayor sea el número de *bits* de la clave menos vulnerable será. No obstante, y aunque sea una mera idea de laboratorio, es cierto que realmente resulta posible descubrirla si se tienen medios, capacidad y, sobre todo, tiempo para ello (años quizá). Hace pocos años se recomendaban algoritmos de sesenta y cuatro dígitos que hubo que aumentar ante la mejora de los métodos de descifrado. En principio, los dígitos pueden aumentar sin fin si los de menor tamaño se vuelven inseguros, aunque la hipotética realización práctica de "computadoras cuánticas" puede reducir de manera considerable el tiempo de descifrado con lo que habría que replantearse de nuevo toda la cuestión.

Este sistema de doble clave aporta gran lentitud (se dice que es cien veces más lento que el sistema de única clave secreta). Esto hace que, en la práctica, dicho sistema se suela utilizar para enviar una de las claves tradicionales o simétricas, procediéndose, a continuación, al envío de la información cifrada con esta clave tradicional. Es decir, que el texto se codifica con un algoritmo de clave simétrica, empleándose un algoritmo de clave asimétrica para remitir aquella clave, la simétrica, al destinatario, que con su clave privada decodificará la clave simétrica que necesita para desencriptar el texto del mensaje.

La importancia y complejidad de la generación y gestión de los actuales sistemas criptográficos han dado lugar a la creación de infraestructuras de clave pública (PKI o *public key infraestructure*), que reúnen los diversos elementos necesarios para la creación de las claves y su administración, además de ir asumiendo nuevas funciones de intermediación, registro o auditoría. Como esquematiza Font (2000, 62), tres son los componentes esenciales de una PKI: la autoridad de certificación (emite los certificados digitales que veremos más abajo), el directorio que contiene

las claves públicas y los certificados, y el *management* del sistema.

3. *Criptografía y seguridad pública*

La encriptación puede originar un choque de intereses entre la garantía de la privacidad y la seguridad pública, pues podría servir para tapar actividades delictivas y/o contrarias a los intereses del Estado. La seguridad pública, el interés nacional, la razón de Estado o la defensa nacional son las razones esgrimidas por las autoridades para supervisar las cuestiones relativas a la criptografía. La problemática es más intensa respecto a la encriptación asimétrica dado que está abierta a más personas por el carácter público de una de las dos claves usadas. Respecto a la simétrica, al producirse en un conjunto cerrado de personas, jurídicamente hablando, o se acepta o se prohíbe (prohibición, por otra parte, de dudosa eficacia). En la asimétrica puede ser un tercero, como un servicio de telecomunicaciones, el que atribuya la clave secreta. Entonces el poder público, en teoría a través de una resolución judicial, puede dirigirse a ese tercero para que descubra la clave y, de esta forma, se pueda proceder a descifrar la comunicación intervenida.

Surgen, así, debates jurídicos que tratan de fijar hasta qué punto es admisible que "la tecnología cree zonas de protección absoluta dentro del derecho al secreto de las comunicaciones" (Rodríguez Ruiz, 1998, 128). Por ello, en diversos países está prohibido el uso de programas de encriptación de mensajes de correo electrónico (como el gratuito que se consigue en Internet PGP o *Pretty Good Privacy*, aunque este programa ya no parece seguro desde que la empresa distribuidora, *Network Associates*, empezara a negar a los usuarios el acceso a su código fuente, por lo que existe el riesgo de que contenga "puertas traseras" al servicio de agencias gubernamentales estadounidenses), además de establecerse controles de muy diverso

tipo, sobre todo en el terreno de la exportación. Es el caso de Australia, Canadá, China, Corea del Sur, Israel o Taiwán. En Europa los intentos de prohibición no han prosperado (como en Holanda), al margen de asistirse a modificaciones legislativas que eliminaban restricciones anteriores (como en Francia en 1996, 1998 y 1999, cuya legislación en la materia era considerada como una de las más represivas del mundo —hasta 1990 la criptografía no fue accesible a la empresa privada—), aunque permanecen restricciones a la exportación en Bélgica o el Reino Unido, entre otros. En la Unión Europea la exportación de medios criptográficos está sujeta al Reglamento CE/3381/94, del 19 de diciembre de 1994, por el que se establece un régimen comunitario de control de las exportaciones de productos de doble uso (un producto de doble uso es cualquier producto que pueda destinarse a usos tanto civiles como militares) y a la decisión 94/942/PESC del Consejo, de la misma fecha, relativa a la acción común adoptada por el Consejo sobre la base del artículo J.3 del Tratado de la Unión Europea referente al control de las exportaciones de productos de doble uso. En Estados Unidos, por su parte, la exportación de material criptográfico avanzado está muy dificultada. Hasta 1996 los medios criptográficos eran considerados armas de guerra, por lo que toda solicitud de exportación debía pasar por la NSA. Desde ese año la exportación de esos productos ha pasado a ser competencia del Departamento de Comercio y entrado en el ámbito normativo de la Export Administration Act, aunque la atribución de las licencias respectivas permanece controlado por departamentos ligados a las cuestiones de seguridad.

En la misma línea de prevención también se sitúan diversos acuerdos internacionales de limitación de productos de doble uso que afectan al cifrado de clave pública, en los que se prohíbe la exportación indiscriminada de cifrado robusto para que no obstaculice la persecución de actividades criminales por parte de las autoridades esta-

tales. En este sentido se puede citar el Acuerdo de Wassenaar, firmado por treinta y un países en 1996 con el objetivo de controlar la exportación de armas convencionales y bienes y tecnologías de uso militar y civil, y limitar, así, la acumulación de armas de destrucción masiva en ciertas regiones susceptibles de violar el derecho internacional.

Además existen propuestas, que en alguno de los casos ya se han llevado a la práctica, dirigidas a que las autoridades públicas tengan medios para, cuando sea preciso, proceder al descifrado. Uno de esos medios es el depósito de las claves privadas que se usan (*mandatary key recovery system* o *key escrowed system*) en un lugar custodiado por un ente público. Así, por ejemplo, en Estados Unidos se tiene el proyecto Clipper que impulsa un *chip* seguro y un sistema de depósito de las claves secretas para que el poder público, llegado el caso, pueda proceder a "abrir" cada *chip*. Cada clave se divide en dos elementos, cada uno de los cuales se deposita en un órgano administrativo (las denominadas agencias depositarias) diferente para su custodia. Cuando se hace necesario descifrar una comunicación, una autorización judicial permitirá juntar los dos elementos de la clave y, así, descifrar. El poder público se asegura que un programa de cifrado no sea utilizado ilegalmente si consigue que sólo circulen programas con un sistema de acceso para ser utilizado por los agentes de la autoridad en caso de necesidad. Es lo que se viene denominando programas con "puerta trasera". La generación de claves con los navegadores más extendidos (*Explorer* de *Microsoft* y *Communicator* de *Netscape*) limita la longitud del correspondiente algoritmo por las exigencias gubernamentales estadounidenses que limitan la exportación de técnicas criptográficas.

Estas propuestas y restricciones originan la lógica reacción de las personas interesadas y defensoras del comercio electrónico y las que hacen prevalecer a toda costa la defensa de la privacidad y de la libertad de comunicación, dando lugar a polémicas que tienen amplia repercusión en

los medios de comunicación (como la que en 1998 enfrentó al presidente de *Microsoft* y al gobierno de los Estados Unidos). La respuesta a esta dialéctica es ciertamente difícil y no vemos que sea posible situarse en una posición intermedia sino necesariamente en uno de los dos polos porque si se articula un sistema como el mencionado del depósito, que, llegado el caso, permita al ente estatal descifrar el mensaje o los datos, se hace prevalecer la idea de seguridad general, y si no se construye tal sistema lo que prevalecerá será la vida privada. En todo caso, nos inclinamos por la segunda opción. Un sistema de depósito puede hacer a la criptografía insegura, con lo que dejaría de tener sentido. Además, los criminales tratarán de emplear claves que nunca registrarán por lo que el permitir a los poderes públicos acceder a las claves secretas no se traducirá en una mayor eficacia en la lucha contra la delincuencia.

En España la opción parece ser el depósito pues el artículo 52.2 de la ya citada Ley General de Telecomunicaciones posibilita "imponer la obligación de notificar bien a la Administración del Estado o a un organismo público los algoritmos o cualquier procedimiento de cifrado utilizado", y el artículo 52.3 establece que los operadores de redes que "utilicen cualquier procedimiento de cifrado deberán facilitar a la Administración General del Estado, sin costo alguno para ésta y a los efectos de la oportuna inspección los aparatos decodificadores que empleen". Estas previsiones podrían dar lugar a una eventual apertura del mensaje sin intervención judicial, lo que sería inconstitucional, aunque esta interpretación la estimamos ciertamente errónea, máxime cuando en el propio precepto se dice que todo ello se hará "de acuerdo con la normativa vigente". La intervención de las comunicaciones sólo puede hacerse por autorización judicial, motivada y basada en la legalidad y proporcionalidad (sentencias del Tribunal Constitucional español 37/1989, fundamento jurídico 8o.; 86/1995, fundamento jurídico 3o.; 49/1996, fundamento jurídico 3o.).

Además, esta obligación de entrega de claves también despierta sombras de inconstitucionalidad por vulnerar el derecho a no declarar contra sí mismo (Ruiz Miguel, 1998, 53).

En todo caso, el medio empleado para realizar una comunicación puede facilitar o dificultar la interceptación pero no puede servir de argumento jurídico, ya que la aproximación a la cuestión de la intervención de comunicaciones tiene que realizarse desde un punto de vista material, teniendo siempre como referente el derecho al secreto de las comunicaciones. La protección de una comunicación se debe producir por sí misma y no porque no esté (o esté) encriptada asimétricamente.

4. *Firma digital y certificado digital*

Existen, además, otros problemas de importancia que afectan a la intimidad en Internet y que también se conectan con la encriptación. Aludimos a las cuestiones que se quieren solventar con la firma digital y el certificado digital, como son la autenticidad e identidad del emisor, y la integridad y confidencialidad del mensaje.

Se suele distinguir entre diversos tipos de *firma digital* o electrónica. Así, por ejemplo, se diferencia entre firma digital y firma digital avanzada, como hace el Real Decreto-Ley 14/1999 que regula en España la firma electrónica. La primera autentica al autor del documento y la segunda hace lo mismo y, todavía más, permite detectar el cambio del contenido del mensaje, o sea, permite constatar la integridad del mismo. De tal modo, el receptor sabrá que el mensaje ha sido alterado o no en la Red. Para realizar una firma digital se pueden emplear diversas técnicas (pluma digital, *password*, biometría digitalizada, escaneo digital de la firma autógrafa, etcétera). En cambio, para realizar una firma digital avanzada se suele acudir a la criptografía asimétrica. Lo primero que se hace es un resumen del contenido del documento aplicando una función *hash* (el algoritmo generalmente empleado es el llamado SHA-1 o *se-*

cure hash algorithm 1). Se obtiene, de este modo, una especie de "extracto", "huella digital" o versión reducida, denominada en inglés *message digest*, consistente en una cadena de *bits* de tamaño fijo que se hace derivar del mensaje. A continuación, a ese extracto digital del mensaje se aplica la clave privada del emisor; así surge la firma digital, que se envía con el mensaje. Cada comunicación que se realice con un mensaje diferente tendrá su propia firma digital. El receptor, con la clave pública que usa el emisor, decodifica la firma digital y obtiene el extracto digital del documento, tras lo cual comprobará si dicho extracto se deriva realmente del mensaje transmitido. Para ello realiza de nuevo dicho extracto a partir del texto que le ha llegado empleando el mismo algoritmo. Si hay coincidencia, el mensaje será el que en verdad ha enviado el emisor. Si el mensaje se hubiera alterado en el camino, aunque sea mínimamente, el extracto no corresponderá al contenido del mensaje, por lo que el receptor sabrá que se ha llevado a cabo tal alteración. La vinculación de la firma con los datos permite detectar las hipotéticas alteraciones de los mismos. Otra opción es que el emisor cifre el documento y su firma con la clave pública del destinatario, con lo que sólo éste, aplicando su clave privada, podrá acceder al mensaje. También se pueden combinar las claves pública y privada de emisor y receptor. Así, la firma digital avanzada supone que al documento que se envía se le estampa un sello electrónico creado mediante criptografía asimétrica. De esta forma, se vincula a alguien a un determinado mensaje.

La firma digital, como vemos, permite saber que un mensaje ha sido enviado íntegramente por un usuario determinado, pero no posibilita garantizar que dicho usuario es quien dice ser y no un impostor, por lo que se hace necesario avanzar un paso más mediante la entrada en escena de un tercero imparcial que vincula una clave pública con un sujeto determinado de forma segura, seguridad en la que confiarán los que contraten con dicho sujeto. Surge

así el *certificado digital* para garantizar la identidad del origen. En efecto, la certeza de la titularidad de la firma electrónica avanzada se consigue gracias al certificado digital que emite una entidad que presta el servicio de certificación, entidades que pueden ser públicas o privadas. Con él se sabrá quien es realmente el que hace la comunicación (la normativa española sobre firma electrónica, ya citada, define el certificado como "la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad", en una dicción que sigue al artículo 2.9 de la directiva europea 1999/93/CE).

Para obtener un certificado digital hay que acudir a una autoridad certificadora, que actúa de tercera parte de confianza (por ejemplo, en España, la Fábrica Nacional de Moneda y Timbre, en virtud de la Ley de Medidas Fiscales, Administrativas y del Orden Social del 30 de diciembre de 1997; o, en el ámbito supranacional, la empresa *VeriSign*, cuya infraestructura de clave pública, de ámbito mundial y que data de 1995, puede ser usada con productos diversos, entre los que se encuentra el programa *Outlook Express* de *Microsoft*). Por lo general, la prestación de servicios de certificación se efectúa en régimen de libre competencia.

El que solicita el certificado debe enviar a la autoridad de certificación sus datos identificativos y su clave pública (normalmente, además de la autoridad de certificación habrá una autoridad de registro encargada de identificar y registrar a los solicitantes de un certificado digital —una sucursal bancaria o una cámara de comercio, por ejemplo—). A continuación se comprueban dichos datos para asegurarse de su certeza. Si son verdaderos, esa autoridad certificadora codifica dicha información (junto con la clave pública del solicitante) con su clave privada, para obtener, de este modo, el certificado digital del sujeto que lo ha solicitado. En las comunicaciones este sujeto enviará dicho certificado digital. El destinatario de los mensajes de dicho sujeto utilizará la clave pública de la autoridad certificadora para decodificar el certificado y obtener los rasgos

identificativos del emisor, que permiten corroborar que la comunicación procedía en realidad de ese determinado emisor. La elaboración de un certificado suele conectarse con el nombre de dominio, cuyos datos están almacenados en registros accesibles públicamente. De esta forma, se exige que el solicitante posea una dirección de correo electrónico que haya sido generada a partir de un dominio registrado. Los certificados se emiten antes de la elaboración de la firma digital y sirven para un número indeterminado de éstas, aunque suelen tener un periodo de validez determinado al constar en ellos el plazo de dicha validez, aunque también habrá otras causas que ponen fin a su vigencia (fallecimiento o incapacidad del signatario, revocación, resolución judicial o administrativa, etcétera).

Los certificados pueden ser de diversos tipos en función del nivel de seguridad al que respondan. *VeriSign* diferencia tres niveles que van de menor a mayor seguridad. En el nivel 1 el certificado se genera con base en la declaración del solicitante sobre el nombre y la dirección de correo electrónico que usa para realizar la solicitud a distancia. El único requisito consiste en que la dirección de correo electrónico sea inequívoca, para lo cual dicha empresa contrasta el nombre del dominio de la cuenta de correo electrónico empleada para la solicitud con el elenco de nombres de dominio registrados. La finalidad de estos certificados es navegar por la *web* e identificar el envío de correos electrónicos. En los certificados de nivel 2 los datos del solicitante son comprobados por la entidad local de registro sin que tampoco sea necesaria la presencia física de dicha persona. Los certificados de nivel 2 se usan para el correo electrónico dentro de una compañía, correo entre compañías o para el acceso *on line* a bases de datos usando el certificado como palabra de paso. Los certificados de nivel 3 se realizan con programas que den suficiente confianza, por lo que pueden utilizarse para cuestiones que exigen mayor seguridad, como las ligadas al gobierno electrónico o la banca en la Red. La escasa seguridad de los

niveles 1 y 2 da lugar a que Galindo los considere "como certificados de demostración, que pretenden popularizar en la medida de lo posible el uso de las técnicas de cifrado" (en Cayón Garrido, 2001, 45).

Así, un usuario puede aplicar a un mensaje que envíe su firma digital o, si quiere aportar confidencialidad al mismo, firmarlo y codificar dicho mensaje con la clave pública del destinatario. El destinatario aplicará su clave privada para hacerlo legible y la clave pública del emisor para revelar la firma digital y conocer su autoría. Un correcto uso de estos sistemas aconseja que cada usuario disponga de cuatro claves, dos privadas y dos públicas, para mejorar la seguridad. Un par de ellas (claves de confidencialidad) se usan para encriptar los mensajes y otro para la generación de las firmas digitales (claves de autenticación). En la práctica la complejidad de todos estos procesos es pequeña dado que los realizan los equipos informáticos directamente.

La directiva europea 1999/93/CE, sobre firma electrónica, trata de homogeneizar la normativa sobre la cuestión en los países de la Unión, ya que entiende que la heterogeneidad de la misma "puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico", además de que "un marco claro comunitario sobre las condiciones aplicables a la firma electrónica aumentará la confianza en las nuevas tecnologías y la aceptación general de las mismas" (considerando 4). Esta directiva ha establecido un sistema de empresas proveedoras de servicios de certificación o terceras partes de confianza organizadas en sistemas voluntarios de acreditación que deberán salvaguardar la seguridad de las comunicaciones electrónicas. En este tema, en Europa, no existe un organismo similar al ICANN sino que son los propios Estados, asesorados por la Unión Europea, los que establecen en su territorio las empresas proveedoras de servicios de certificación a través de la pertinente normativa. Surgen tres tipos de sujetos: los órganos de acreditación de prestadores de

servicios y certificación de productos, las entidades de evaluación y el órgano independiente de acreditación de las entidades de evaluación. No obstante, en este ámbito también se hallan presentes códigos de práctica, como el de la citada empresa *VeriSign*. A pesar de la recomendación de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre la neutralidad tecnológica, y de la propia directiva de la Unión Europea sobre firma electrónica (se impusieron, en este sentido, las tesis de Finlandia, Holanda, Reino Unido y Suecia), diversos ordenamientos jurídicos nacionales del viejo continente (como el italiano —Decreto del 10 de noviembre de 1997—, el alemán —Ley del 13 de junio de 1997— o el español —Real Decreto-ley 14/1999—) se inclinan hacia la criptografía asimétrica de clave pública para la realización de estas figuras.

V. Otras agresiones

Las agresiones a la intimidad distintas de la interceptación de mensajes tienen, a veces, más difícil respuesta. Así, ante la *elaboración de perfiles de los navegantes* un usuario "medio", o sea, no experto, poco puede hacer salvo acudir a una computadora diferente a la suya. Un gran número de empresas tiene sumo interés en conocer los hábitos de navegación del internauta por razones publicitarias o de cualquier otro tipo, aunque difícilmente son previsibles las consecuencias que siguen a la elaboración de un perfil. La navegación por la Red origina un rastro perfectamente detectable, que se traduce en ciertos datos que sirven de base para la construcción del perfil (al margen de que el proveedor de acceso siempre puede saber por donde está navegando uno de sus clientes sin necesidad de buscar con medios complejos dicho rastro). A veces los datos que se extraen de los equipos informáticos son necesarios, como los datos técnicos que un suministrador obtiene del equipo informático que le está solicitando bajar

un programa y que son precisos para bajar dicho programa ajustado a una configuración determinada. En cambio, en la mayoría de las ocasiones la justificación no existe. Antes de la elaboración de perfiles pudieron haber actuado programas rastreadores o *sniffers* en busca de direcciones IP violables. Al contar con este dato se tiene localizado al usuario, que será detectado cuando entre en una página *web* determinada, aunque el asunto se complica si la dirección IP que se usa es móvil y no fija. En efecto, hay supuestos en los que al usarse una dirección IP móvil no será posible asociarla a una determinada persona, con lo cual no se podrá elaborar el perfil de la misma. Igualmente, las ya comentadas *cookies* permiten recabar datos para construir los perfiles, del mismo modo que acceder a través del correo electrónico a boletines de información o a grupos de discusión, aunque todos estos supuestos encuentran problemas cuando se usan direcciones IP móviles, que sólo podrán ser relacionadas con usuarios concretos si el proveedor de acceso colabora en la elaboración del perfil y busca en sus registros qué cliente ha estado usando esa IP en el momento que interesa.

Si el internauta no adopta ninguna medida de bloqueo las *cookies* se irán almacenando en el directorio respectivo de su disco duro sin parar. Llegará un momento en que en dicho directorio existirá una información cabal de sus preferencias de navegación. A pesar de que las exigencias de la intimidad llevan a que sea necesario el consentimiento del afectado para recoger y usar sus datos personales, la práctica nos muestra cómo esto no suele producirse. Incluso hay usuarios que ignoran su propia existencia. Como mucho, lo que puede suceder es que el navegante sea avisado de la recepción de la *cookie*, pero no lo va a ser del tratamiento de los datos que contiene. El servidor reconoce con rapidez nuestras *cookies* y, a través de ellas, las páginas *web* visitadas. Incluso hay sitios cuya publicidad correrá a cargo de centrales interactivas que con bastante probabilidad realizarán procesos de agregación

de datos de los usuarios. La *cookie* puede informar de multitud de aspectos en función de lo que pretendió el diseñador de la misma, incluyendo componentes de *hardware* del equipo o la existencia de *software* pirata en dicho equipo. Para enfrentarse a los problemas de las *cookies* de nuevo resulta en algún caso de suma utilidad acudir al cifrado y a las firmas encriptadas. Aunque una ayuda más cómoda y muy efectiva es usar programas que bloquean la entrada de *cookies* en el ordenador, además de avisar cuando se producen intentos de seguimiento de rastros de navegación. Hablamos, por ejemplo, del gratuito IDcide Privacy Companion. En los propios navegadores de uso más extendido hay posibilidad de dificultar el almacenamiento de *cookies*. Así, en el *Internet Explorer* se puede activar el menú Herramientas, allí buscar Opciones de Internet, ahí, a su vez, escoger Seguridad, donde se puede personalizar el nivel de seguridad. En el *Netscape Navigator* hay que ir al menú Edición, escoger Preferencias y, ahí, las Avanzadas, donde hay la opción para aceptar o rechazar todas las *cookies* o aceptar sólo aquellas que se devuelven al servidor originario.

El internauta, asimismo, puede tomar diversas precauciones con base en la información que proporcionan cierto tipo de programas que le transmiten las huellas electrónicas que va dejando su navegación. Igualmente, para enfrentarse a estas agresiones el usuario puede emplear el anonimato (o un seudónimo). La navegación anónima es posible si nos conectamos previamente a una página que no da información del usuario y, a partir de ahí, comenzamos la navegación (por ejemplo, www.anonimyzer.com), si bien es cierto que en diversas ocasiones, por razones prácticas, no es posible actuar anónimamente, como, por ejemplo, a la hora de comprar por la Red, tal y como apunta Van Allen (2002, 1). El supuesto lógico para intentar aplicar estas medidas de autoprotección es el conocimiento de la existencia de estos peligros, lo cual no siempre sucede, por lo que un régimen de garantía basado exclusi-

vamente en tales medidas resulta insuficiente. Habría que establecer, por ejemplo, la obligatoriedad de que la configuración por defecto de los *software* de navegación rechazase las *cookies*, lo que tendría que articularse a través de un acuerdo internacional o por medio de medidas de autorregulación de las empresas fabricantes de ese tipo de *software*. Sin embargo, surge un problema adicional: la existencia de páginas que no dejan ser visitadas si el internauta no admite *cookies*. Esta posibilidad, si tiene propósito legítimo, es aceptada por la directiva 2002/58/CE en su considerando 25.

El temor excesivo que están despertando las cookies está dando lugar, como afirma Javier Ribas, a que "su uso se haya satanizado hasta el punto de que algunos autores han interpretado erróneamente que la nueva directiva 2002/58/CE las prohíbe expresamente", lo que no es cierto porque, como ya hemos visto, en su considerando 25 se reconoce que las *cookies* pueden constituir un instrumento legítimo y de gran utilidad. A esta idea el autor citado añade que "para analizar si el usuario tiene conocimiento del uso de *cookies* debería bastar el texto que habitualmente aparece en los sitios *web*, informando sobre la política de la empresa en materia de intimidad y datos personales" (Javier Ribas, http://landwell.blogspot.com/, el 18.02.2002). La citada directiva exige que los usuarios tengan "la posibilidad de impedir que se almacene en su equipo terminal" una *cookie* o un dispositivo semejante, lo que es "particularmente importante cuando otros usuarios distintos al usuario original tienen acceso al equipo terminal" (de nuevo el considerando 25).

Un par de cuestiones más respecto a las *cookies* (aunque volveremos sobre ellas en el último epígrafe de este capítulo): por sí mismas no parecen suponer agresión ninguna ya que, aunque el secreto de las comunicaciones se extiende a circunstancias externas tales como la identidad de los comunicantes, el proceso de entrada de *cookies* en el equipo informático del navegante no tiene que ver con

el envío e hipotética interceptación de un mensaje a un destinatario concreto. Lo que se almacena es la visita a una página *web*, cosa que no entra en el concepto de comunicación que sirve para construir el derecho al secreto de las comunicaciones. El problema estará en el mal uso que se haga de las *cookies* y no en las *cookies* mismas. Además, la problemática de las *cookies* no se agota en los perfiles del navegante, ya que puede proporcionar información que no se usa para establecer perfiles sino para, por ejemplo, realizar fraudes con el número de tarjeta de crédito que almacena la *cookie* o para conseguir la clave de acceso a determinadas páginas suplantando al verdadero suscriptor.

Pero para elaborar perfiles a veces no son necesarias las *cookies*. Existen maneras también ocultas de seguir el rastro del navegante. En este sentido, tenemos los denominados fallos del navegador (*web bugs*), que hacen posible que un servidor *web* controle al usuario. Estos fallos pueden tomar la forma de un pequeño elemento gráfico en una página *web*, incluso oculto por ser del mismo color que el fondo de dicha página. Al tomar la dirección IP del usuario para enviar el gráfico, el servidor puede llevar a cabo un seguimiento de la navegación posterior.

Otra forma de realizar un perfil de una persona es averiguar su dirección de correo electrónico, que por si sola proporciona datos como el de la empresa o institución en la que trabaja o la de su país. Incluso, puede ofrecer datos sobre el nombre o apellido de esa persona. El perfil puede ir mucho más allá cuando se analizan los usuarios que pertenecen a uno o a otro grupo de discusión o, incluso, por las visitas a los *chats*.

Igualmente, los datos de conexión, que recaban los proveedores de acceso, son también útiles para estos fines pues ofrecen datos del emisor y del destinatario de un correo, fechas y horas, el uso concreto de la Red (páginas *web* visitadas, frecuencia, duración de las visitas), etcétera. Para estos proveedores o prestadores de servicios de Internet elaborar un perfil resulta sumamente sencillo, ya

que saben sin problemas quien es la persona que ha contratado con ellos el servicio. En cambio, los que gestionan los servidores *web* tendrán que buscar y operar sobre las *cookies* para trazar estos problemáticos perfiles.

Por su parte, las *entradas al disco duro* se llevan a cabo con programas denominados en la jerga "troyanos" y "gusanos", también aludidos más arriba y que se ven precedidos por la actuación de un *sniffer*. En estas entradas, que quizá sean la agresión más importante, son muchas las variables que influyen facilitándolas o entorpeciéndolas. Los medios de prevención pueden ser contraseñas y códigos de acceso cuya eficacia dependerá del grado de conocimientos, del tiempo y de los medios a disposición del intruso, y también de lo precavido y de los conocimientos informáticos del titular del ordenador agredido. Estos ataques se ven facilitados por la costumbre de muchos usuarios de utilizar claves de acceso fáciles de adivinar. Introducir letras y números en la clave o establecer una fecha de caducidad para la misma son dos maneras simples de dificultar la labor al agresor. De igual manera, el sistema operativo del ordenador atacado también influye pues no es lo mismo la seguridad de un UNIX o de un *Windows* NT que la seguridad (o inseguridad más bien) de un *Windows* 95 o 98. En todo caso, las entradas al disco duro tienen que hacerse desde la red local en la que se halla el ordenador atacado. Igualmente, se hace necesario recordar que los avances futuros pueden cambiar la fisonomía de este tipo de agresión, ya que el disco duro quizá desaparezca para ser sustituido por una memoria "viva" en la Red. La directiva 2002/58/CE es taxativa en esta cuestión al indicar que "los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida" (considerando 24).

Es indudable que estos ataques son más graves si se dirigen contra una computadora que se dedica a gestionar

el tráfico de Internet, lo que se llama, como dijimos en el capítulo primero, "encaminador" o *router*. El pirata que la controle, como señala Vila Sobrino, "podría espiar toda la información que fluye a través del mismo, dar a su propio ordenador la dirección que él quisiese, suplantar a otros ordenadores" o colapsar la Red (en Gómez Segade/Fernández-Albor/Tato, 2001, 62). Esta es la razón de las especiales medidas de seguridad que rodean a los "encaminadores", como el acceso mediante tarjetas o el empleo de medidas biométricas.

La *suplantación de personalidad* es un fenómeno que se puede dar con relativa facilidad en la Red, viéndose agredida la intimidad del suplantado por el simple hecho de suplantarla aunque no se persiga nada perjudicial. Esto ocurre, por ejemplo, cuando se envía un correo electrónico usando la cuenta de un tercero o cuando se usa la dirección IP que tiene asignado otro ordenador. Un tipo diferente de suplantación es aquella con la que se suplanta la identidad de una computadora, lo que puede ser realmente grave ya que es factible explotar su credibilidad. En efecto, entre los equipos informáticos de una red hay diferentes niveles de credibilidad. Si el pirata suplanta a una computadora de credibilidad alta, que sea considerada "máquina segura", tendrá más facilidades para acceder a cuentas de usuarios, ya que si la computadora que es "máquina segura" tiene cuenta en otro equipo informático, éste no le solicitará la clave de acceso. Para evitar este riesgo los administradores de red deben ser precavidos a la hora de catalogar un equipo como "máquina segura".

Asimismo, otro de los problemas que están a la orden del día es la posibilidad de *captar datos* sin consentimiento del afectado, datos que pueden ser objeto de tratamiento automatizado para configurar los citados perfiles personales vinculados a una dirección electrónica.

De igual forma, no hay que olvidarse de que los datos personales no son sólo acumulados y registrados, sino que también se procede a su *transferencia*, que puede ser in-

cluso venta o alquiler, entre empresas sin autorización de los afectados. Este es otro problema grave que ocurre con demasiada frecuencia (las empresas estadounidenses *DoubleClick* y *Yahoo* están siendo investigadas por tales hechos). Empresas de publicidad y de *marketing* directo cruzan en más ocasiones de las que se supone sus bases de datos personales construidas gracias a los perfiles de navegación que elaboran. Del mismo modo, esas empresas realizan en ocasiones un *uso indebido de los directorios de correo electrónico y/o de las listas de usuario.*

El *hostigamiento electrónico* puede ser de tal calibre que merezca la consideración de agresión a la intimidad del individuo que lo padece. Una forma típica de semejante hostigamiento es el *spam* (también denominado *spamming* o *junk e-mail*), consistente en el envío masivo y no solicitado de mensajes publicitarios por correo electrónico. La directiva 2000/31/CE, sobre comercio electrónico, afirma categóricamente que "el envío por correo electrónico de comunicaciones comerciales no solicitadas puede no resultar deseable para los consumidores y los prestadores de servicios de la sociedad de la información y trastornar el buen funcionamiento de las redes interactivas" (considerando 30). En el artículo 7o. establece que "los Estados miembros que permitan la comunicación comercial no solicitada por correo electrónico garantizarán que dicha comunicación comercial facilitada por un prestador de servicios establecido en su territorio sea identificable de manera clara e inequívoca como tal en el mismo momento de su recepción", a lo que se añade que "los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria (*opt-out*) en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten". En Francia la Commission Nationale Informatique et Libertés (CNIL) se ha pronunciado expresamente en fa-

vor de la solución *opt-out*. Como la directiva mencionada permite a los Estados de la Unión Europea establecer disposiciones más protectoras con el consumidor que las reguladas por la propia directiva (artículo 14), algunos ordenamientos, como el belga o el italiano, han adoptado la solución *opt-in*, que consiste en prohibir el envío de mensajes publicitarios salvo que haya una autorización previa del destinatario. A su vez, la directiva 2002/58/CE, en su artículo 13, sigue esta línea más garantista al establecer que la utilización del correo electrónico con fines de venta directa sólo se podrá autorizar con consentimiento previo (a lo que también responde el artículo 21 de la Ley española 34/2002, servicios de la sociedad de la información), aunque cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio,

> esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.

En los países europeos tiene creciente importancia el acceso no autorizado a sistemas informáticos, la alteración de los mismos, el apoderamiento de ficheros, la interceptación ilegal de correo electrónico y la intrusión informática, que pueden entrar dentro del tipo penal de descubrimiento y revelación de secretos. Los medios informáticos y tecnológicos, incluida la encriptación, son cada vez más habituales en la delincuencia organizada; esta tendencia también se manifiesta en actividades terroristas. Por ello los poderes públicos europeos muestran bastante sensibilidad por toda esta compleja problemática. Así, la reco-

mendación que el Comité de Ministros de la Unión Europea dictó el 19 de febrero de 1999 para proteger la intimidad de los usuarios de Internet aconseja que se usen todos los medios disponibles de protección, como la criptografía, los códigos de acceso al ordenador personal, programas que informen de las huellas electrónicas que un navegante deja como rastro, dar preferencia a los dominios que acumulen pocos datos o a los que se pueda acceder anónimamente, buscar medios técnicos que proporcionen el anonimato, si éste no es posible emplear un seudónimo, dar al servidor sólo los datos estrictamente necesarios, o preguntar al servidor qué datos obtiene y con qué finalidad.

VI. La protección de datos

Las cuestiones referidas a la protección de datos requieren un tratamiento peculiar en el campo de las telecomunicaciones dado que las mismas conllevan un riesgo adicional en esta temática, cuanto más las telecomunicaciones electrónicas. Diversos aspectos conectados con esta problemática ya han sido aludidos con anterioridad, pero hemos considerado adecuado abrir ahora un apartado específico sobre protección de datos antes de continuar. En principio, la protección de datos personales opera al margen de la circulación de los mismos, por lo que su tratamiento tiene autonomía respecto a las cuestiones que plantea Internet. No obstante, es habitual que el ámbito de aplicación de la protección de datos sea delimitado de forma amplia en lo relativo a los aspectos informáticos, con lo que la Red entra de inmediato en escena. Así, la normativa de protección de datos hay que considerarla aplicable a los datos personales que circulan por Internet. Y no sólo eso, sino que también resulta común, como ya observamos en el apartado II de este capítulo, reconducir los problemas que genera la intersección entre intimidad e informática a las cuestiones de protección de datos, lo que entendemos como un reduccionismo que desconoce la realidad del pro-

blema, aunque bien es cierto que la regulación de la protección de datos se sitúa desde el punto de vista histórico "en el comienzo del derecho a la información" (Hoeren, 2001, 57). La Red es un nuevo reto para esta problemática hasta el punto de que "la protección de las bases de datos ha adquirido con Internet una dimensión global" (Lehmann, 1998, 952). El principio de referencia es el principio de universalidad de la protección de datos. Por paradójico que resulte, las sociedades democráticas, "amparándose en la legitimidad que les atribuye la defensa de los intereses generales," piden y demandan, "cada vez con más insistencia, tener acceso a datos personales" (Álvarez-Cienfuegos, 1999, 22).

Una aproximación conceptual que nos sirve de apoyo para ver esta amplitud de aplicación nos la puede proporcionar la Ley española de protección de datos de carácter personal (Ley Orgánica 15/1999, del 13 de diciembre, que desarrolla el ya citado artículo 18.4 de la Constitución española). Aquí se entiende por datos de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables" (artículo 3o.), "registrados en soporte físico, que los haga ser susceptibles de tratamiento" (artículo 2.1). Se considera tratamiento las "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". Si el dato es de carácter personal, esta Ley no establece limitación de ningún tipo por razones de materia. Tampoco hay excepciones con base en el soporte. Sin embargo, sí las hay por la finalidad de los ficheros de datos (doméstica) o por razones de interés general (materias clasificadas, delincuencia organizada, terrorismo). Estas previsiones españolas hay que enmarcarlas en un contexto más amplio, ya que la normativa de la Unión Europea ha creado un espacio común en el que la protección de datos está regida por

principios homogéneos. En este sentido el documento denominado Carta de los Derechos Fundamentales de la Unión Europea (que todavía carece de valor normativo) establece, en su artículo 8.1, que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan". La sentencia del Tribunal Constitucional español 292/2000, del 30 de noviembre, apunta que

> el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar 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 uso.

Así, los proveedores de acceso a Internet (y los operadores que presten servicios de telecomunicaciones) deben garantizar, en el ejercicio de su actividad, la protección de datos de carácter personal. La Ley española 11/1998, General de Telecomunicaciones, dispone en su artículo 50 que "los operadores que presten servicios de telecomunicaciones al público o exploten redes de telecomunicaciones accesibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal". El concepto de operador de servicios de telecomunicaciones hay que entenderlo en sentido amplio de manera que englobe a todos aquellos que intervengan en el proceso de telecomunicación, con lo que la temática de Internet entra en el mismo. Por ello, les son aplicables los principios y deberes vigentes en la materia. En este sentido podemos citar los siguientes principios: el de precaución a la hora de recoger y tratar los datos, el de adherencia del dato a la finalidad para la que fue recogido, el de lealtad y licitud en su recolección, el de calidad (los datos tienen que estar al día), el de pertinencia, el de seguridad, el de consentimiento y el de responsabilidad por el uso inadecuado de los datos de carácter personal. Las obligaciones

aluden al secreto y a la necesidad de establecer adecuados estándares de seguridad, que habrá que juzgar con base en el riesgo existente, lo que convierte al principio de proporcionalidad en el criterio hermenéutico a tener en cuenta. Asimismo, hay que considerar que el usuario ostenta el derecho a ser informado, el derecho de acceso, rectificación y cancelación de los datos, y el derecho de oposición a que sus datos personales sean puestos en circulación en la Red. La información al afectado debe ser precisa, expresa e inequívoca sobre la existencia del fichero, su finalidad y destinatarios, las consecuencias de la obtención de los datos o de la negativa a facilitarlos, la posibilidad de ejercitar el derechos de acceso, rectificación y cancelación, y sobre la identidad y dirección del responsable del tratamiento de los datos. Los operadores podrán tratar los datos de los usuarios para cubrir las necesidades del tráfico del servicio y la facturación (número del abonado, dirección, tipo de equipo terminal, número de unidades que deben facturarse, número de destino, hora de comienzo de la conexión, duración, fecha, etcétera), si bien una vez que transcurra el plazo para impugnar la factura o exigir su pago los datos deberían destruirse. El tratamiento de datos con fines comerciales debe exigir siempre el consentimiento previo del afectado.

La realidad nos muestra cómo estas cuestiones son vulneradas en Internet. Es más, la difusión por la Red se entiende que nunca es un acto neutro (Féral-Schuhl, 2001, 2). Ya resulta más que conocido que "la tecnología —como apunta Llaneza González (2000, 263)— permite obtener, aplicar, modificar o alterar, borrar, extraer, tratar, ordenar, generar, difundir y almacenar datos de manera prácticamente ilimitada, tanto de forma legal como ilegal". Y no sólo eso, sino que "los datos ofrecidos por los interesados para obtener determinados servicios son tales, por cantidad y calidad, que determinan la posibilidad de toda una serie de empleos secundarios" (Fernández Esteban, 1998, 138). Los mayores problemas los encontramos en el ámbito mer-

cantil, ya que los datos no sólo se buscan para asegurar la correcta finalización de una transacción comercial, para la que puede ser necesaria, por ejemplo, la dirección del usuario, sino que también se acumulan "para predecir las necesidades de los clientes" (Gringas, 2003, 331). De ahí se pasa a vender o alquilar los datos a otras empresas para ayudarlas a "predecir las necesidades de sus clientes" (*idem*).

Particular relieve cobran, en este sentido, las ya aludidas *cookies*, que entran en la computadora sin consentimiento del usuario y, de haberlo, con una información que se limita a la simple recepción de la *cookie* y no acerca del tratamiento de los datos que contiene. Si la *cookie* recoge el nombre del navegante, cuando éste ha personalizado su navegador, se convierte en un dato personal. Además, la dirección IP que la *cookie* puede dar también del navegante permite que sea identificado y, así, de nuevo, los datos recabados se convierten en datos personales y no anónimos. Si la dirección IP es móvil, el servidor *web*, en principio, no podrá identificarlo, pero sí el proveedor de acceso porque fue el que facilitó esa dirección IP a ese cliente en un determinado momento que tendrá registrado, aunque hay que presuponer que el proveedor de acceso no obtendrá la *cookie* (salvo que penetre ilegalmente en el equipo del usuario) y el dato, al no ser asociado a una persona identificable, no será personal. Cuando el proveedor de acceso borre los datos de la sesión del *log* del sistema ya no habrá manera de relacionarlos (el *access log* es un archivo que registra la actividad de un servidor). Está claro que la acumulación de datos sobre la navegación sin que medie un consentimiento inequívoco del navegante viola los principios que rigen la protección de datos. En la misma línea de inadmisibilidad se sitúan la ya vista elaboración de perfiles del navegante y la habitual cesión de datos que se opera en la Red de unas empresas a otras, sin que exista, tampoco, consentimiento inequívoco del afectado. A veces, da la impresión que el acceso gratuito que da un presta-

dor de servicios tiene como contraprestación el uso con fines comerciales de los datos de conexión. Asimismo, hay empresas que sólo prestan sus servicios si el cliente acepta la entrada de *cookies*. El salto de los límites estatales que se produce en Internet dificulta la persecución por parte de las autoridades nacionales de las habituales infracciones referidas a la captura, trato y uso de datos personales.

A pesar de las cautelas que se pueden aplicar en esta cuestión, los riesgos ya vistos que para la intimidad supone Internet obligan a estar especialmente atentos. Es la misma percepción que tiene el Grupo de Trabajo sobre protección de datos del artículo 29 (es el Grupo del artículo 29 citado más arriba), que propone incidir en una mayor conscientización y formación de los usuarios de la Red, conseguir una legislación en la Unión Europea más coherente y coordinada, desarrollar tecnologías que favorezcan la intimidad (anonimato, dificultar la gestión de datos personales por parte de terceros) y establecer mecanismos que favorezcan el control y que estén dirigidos por las autoridades de protección de datos, mecanismos complementados por medidas de autoevaluación sobre la fiabilidad del tratamiento de este tipo de datos. La supervisión de una autoridad independiente también consta de forma expresa en el artículo 8.3 de la Carta de los Derechos Fundamentales de la Unión Europea.

A mayor abundamiento cabe recordar que las bases de datos actuales proporcionan una información cualitativa de la que carecían las antiguas, ya que pueden incorporar elementos de identificación del individuo tales como la voz o códigos genéticos.

En esta temática conseguir códigos de conducta que versen sobre el tratamiento y almacenamiento de los datos personales se nos antoja muy interesante. De este modo, como señala Ureña, el propio mercado expulsaría "a todos aquellos que no fuesen respetuosos con los datos de carácter personal de las personas que se asoman a Internet"

(en Cayón Garrido, 2001, 138). España ha sido el primer país de la Unión Europea en el que ha existido un código ético de protección de datos elaborado por la Asociación Española de Comercio Electrónico; pero no nos engañemos ya que ello no es ni será suficiente. El control público no debe dejar de ejercerse. En este sentido, el autor citado aboga por algún tipo de acuerdo o convenio internacional que sirva para aportar principios comunes. En esta línea se muestra el Consejo de Estado francés, que en un informe sobre Internet y redes digitales, del 8 de septiembre de 1998, después de señalar los beneficios, en la protección de los datos personales, de los mecanismos de autorregulación que asocien a los actores económicos y a los usuarios, alude a la necesidad de definir a nivel mundial un *corpus* mínimo de principios de protección de los datos y de establecer una coordinación de los Estados para perseguir y reprimir las eventuales violaciones. Los límites de un enfoque nacional se verían, así, contrarrestados. Una cuestión diferente es la dificultad de cerrar estos acuerdos internacionales habida cuenta de las diferentes posiciones que en la materia sostienen los distintos ordenamientos, unos más garantistas (como los europeos) y otros más flexibles (como el estadounidense).

Es una idea recurrente considerar que en la sociedad actual la información es poder. Entre esa información una de las más valiosas es la que alude a los datos de carácter personal, que con Internet pueden ser tratados, permítasenos la hipérbole (aunque quizá no lo sea tanto), de manera ilimitada. La percepción de semejante cuestión despertó un temprano interés en organismos diversos, como lo prueba el hecho de que ya en 1981 el Consejo de Europa aprobara el Convenio 108, aludido anteriormente, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. En el seno de la Unión Europea también hemos citado ya la normativa específica sobre la cuestión (las directivas 95/46/CE, 97/66/CE y 2002/58/CE —esta última sustituirá a la se-

gunda el 31 de octubre de 2003—), que protege la intimidad en las telecomunicaciones y que es totalmente aplicable a Internet. La directiva 2000/31/CE, sobre el comercio electrónico establece expresamente que ambas directivas son "enteramente aplicables a los servicios de la sociedad de la información" (considerando 14). A su vez, la directiva europea 1999/93/CE, sobre firma electrónica, establece en su artículo 8o. que "los Estados miembros velarán por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos establecidos en la directiva 95/46/CE", y "por que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales directamente del titular de los datos o previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado". El interés por alcanzar en Estados Unidos un nivel de protección de datos similar al europeo dio lugar, en julio de 2000, a la suscripción de un acuerdo entre la Comisión Europea y la administración estadounidense sobre los principios de "puerto seguro" (*safe harbour*). A diferencia de lo que sucede en Europa la tradición estadounidense en este sentido descansa sobre todo en la autorregulación. Por ello, a lo que se comprometen las autoridades estadounidenses es a elaborar una lista de empresas que cumplen con los requisitos de seguridad establecidos al efecto. Las empresas autocertifican anualmente el cumplimiento de tales medidas, lo que origina el riesgo de que a esas empresas se les transmitan datos desde Europa porque alegan cumplir los requisitos cuando en realidad no los cumplen tal y como se refleja en una verificación *a posteriori*. Pese a ello, la nueva normativa europea sobre privacidad de datos ha originado, otra vez, desacuerdos con la administración Bush, menos de un año después de llegar a la solución *safe harbor*.