LA LABOR DE LA COMISIÓN ESPECIAL DEL SENADO ESPAÑOL SOBRE REDES INFORMÁTICAS CON RELACIÓN AL DERECHO A LA INTIMIDAD (*)

JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ (**)

SUMARIO:

(*) El presente trabajo se basa en la ponencia que con el mismo título se presentó en el Congreso «Le nuove frontiere dei diritti fondamentali», celebrado en Siena el 14 y 15 de abril de 2000.

(**) Profesor de Derecho Constitucional. Universidad de Santiago de Compostela.

«El tiempo no se detiene y es necesario subirse, cuando todavía es posible, al tren de la modernidad»

I. Introducción

§1. El progreso técnico de los últimos años ha permitido alcanzar unos logros que resultaban inimaginables no muchas décadas atrás, configurándose, así, un cambio histórico que subvierte realidades sociales y económicas. Estamos en la Sociedad de la Información (1) en donde ésta, la información, se configura como un elemento clave de poder que se demanda, se ofrece, se consume, se procesa, se almacena y se lucha por él, preferentemente en forma digitalizada, o sea, convertida en números (en bits) para ser transmitida. El avance de la técnica ha tenido múltiples repercusiones en campos muy diversos que quizá sólo encuentren parangón en las consecuencias que en su día originó la Revolución Industrial. Incluso se ha dicho, siendo un tanto hiperbólicos, que no asistimos ni a una revolución ni a un cambio de era sino a un cambio de estadio de la humanidad (el «Infolítico») en el que no se trabaja con átomos sino con realidades intangibles. En el marco de estos avances adquiere especial protagonismo Internet, la red de redes, el estandarte de este cambio, que trae consigo unas dosis de interactividad, mundialización, conectividad y globalización sin precedentes hasta el momento. El Estado se ve superado por un fenómeno que llega a escapar de su control. Al mismo tiempo, Internet lleva consigo unas sombras todavía sin disipar como la banalización producida por las enormes masas de información que circulan por la red (basadas en el diseño y en la

(1) Escobar de la Serna subraya como factores que caracterizan a esta «sociedad» la aparición de una serie de medios técnicos de transmisión y de información, que provocan «numerosos efectos sobre el comportamiento individual y colectivo y sobre la formación de hábitos culturales» (Escobar de la Serna, Luis (coord.), *Sociedad, Información y Constitución*, Universitas, Madrid, 1999, pág. 54).

forma antes que en el fondo, y rindiendo tributo a lo cuantitativo, que se impone sobre lo cualitativo), el caos disfuncional, el determinismo técnico, la homogeneización que agrede y empobrece al pluralismo cultural, la dependencia y una tendencia al aislacionismo social que podría tacharse de deshumanizante (un reciente estudio de la Universidad de Stanford, realizado por Norman NIE, indica que los internautas más asiduos tienden a prescindir de amigos y familia; un estudio que está en la línea de otro anterior de la Universidad Carnegie Mellon en el que se señalaba la correlación directa entre horas de Internet e incidencia de cuadros depresivos).

Los rasgos que hacían inteligible el trabajo de la Sociedad Industrial, o sea, el espacio y el tiempo, pierden importancia en la Sociedad de la Información, en la que lo relevante será el resultado y no el período temporal que se dedique a ello ni el lugar desde donde se lleve a cabo. El comercio electrónico abre un conjunto de posibilidades con transcendencia en contextos y niveles muy diferentes, construyéndose desde diversas ópticas una mutación cultural de igual o mayor transcendencia que la técnica.

El mundo jurídico no ha sido una excepción en este panorama de transformaciones y cambios. Se ha visto afectado por realidades nuevas a las que se tiene que enfrentar, a veces, con suma dificultad puesto que las viejas y clásicas categorías del Derecho no son plenamente operativas en la Sociedad de la Información o en el Estado postindustrial. A estos retos hay que responder con prontitud y diligencia para seguir cumpliendo con el fin de regular la vida en sociedad con eficacia y justicia, un fin que, pese a todos los cambios, sigue siendo el referente a tener en cuenta. Ello adquiere renovada relevancia en el campo de los derechos fundamentales dada la posición que los mismos ostentan en los actuales sistemas democráticos. Su garantía y tutela exigen mantener plenamente operativos mecanismos suficientemente eficaces ante los nuevos peligros que los avances técnicos suponen. Entre ellos, el derecho a la intimidad requiere una especial consideración por la intensa amenaza que para el mismo supone Internet. El Estado, como indica ÁLVAREZ-CIENFUEGOS, debe asumir una posición beligerante en la defensa de los derechos de la persona, no permaneciendo ajeno a la «tensión dialéctica entre consumo de información y defensa de la personalidad» (2).

---

(2) ÁLVAREZ-CIENFUEGOS SUÁREZ, José María, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona, 1999, pág. 14.

En los últimos meses hemos contemplado 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» (esta red es capaz de acceder a toda la información transmitida vía Internet, correo electrónico, fax y teléfono), el centro de control de correo electrónico que está instalando el servicio de contraespionaje británico del M15, o los problemas de seguridad de alguna empresa de telefonía, al margen de los periódicos cuadros de pánico por mor de un nuevo y presuntamente catastrófico virus (cada mes surgen ochocientos nuevos virus, estando contabilizados 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 concebido para una realidad bien distinta a la actual. Nuevas respuestas, por lo tanto, parece ser lo que hay que reclamar, sin renunciar a las categorías existentes que pueden seguir siendo operativas con la calificación de principios. Según un informe del Parlamento Europeo conocido en febrero del año 2000, la confidencialidad en Internet es mucho menor de lo que se pensaba ya que todos los correos electrónicos codificados por Microsoft, Netscape y Lotus pueden ser descifrados por un órgano de espionaje norteamericano llamado Agencia de Seguridad Nacional (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, acceso que con ciertas técnicas sigue siendo posible.

II. Origen y fines de la Comisión

§2. La Comisión Especial de estudio sobre las posibilidades y problemas de las redes informáticas (que es su nombre oficial, aunque popularmente se le conoció como Comisión de Internet) se constituyó el 24 de marzo de 1998 en el Senado español. Una moción del Pleno de dicho órgano, aprobada por unanimidad el 24 de febrero de ese mismo año, había previsto su formación. En la solicitud de creación de dicha Comisión se citaban los ámbitos político, jurídico y social como los de referencia para

abordar las posibilidades y problemas que «plantean y pueden plantear en el futuro el desarrollo y la universalización de las redes informáticas». Este tipo de comisiones especiales está previsto en el art. 59.1 del Reglamento del Senado con la finalidad de realizar encuestas o estudios sobre cualquier asunto de interés público, que precisamente también es el objeto de las comisiones de investigación. En nuestro caso se perseguía efectuar un detallado examen sobre las consecuencias políticas, económicas, sociales, culturales y tecnológicas del fenómeno de Internet.

Los solicitantes fundamentan su petición de constitución de la Comisión de una forma muy genérica subrayando la importancia que atesora el tema que se quiere abordar. «El espectacular desarrollo de las redes informáticas —afirman— está produciendo innumerables beneficios y, desde luego, una incipiente transformación de nuestros hábitos laborales y sociales». Consideran la cuestión complicada desde el punto de vista jurídico-político dado que «el "espacio informático" constituye una "tierra de nadie" en la que ningún Estado tiene capacidad de actuar por sí solo». De la realidad virtual se derivan con frecuencia «efectos en la vida "real" y cotidiana de las personas». De este modo, citan, a título de ejemplo, cómo se producen «contratos y acuerdos con trascendencia jurídica realizados en la red, delitos cometidos a través de la red o vulneraciones de derechos ocasionadas dentro» de la misma. Así, con la creación de esta Comisión, España se incorpora al proceso de reflexión política en la materia, proceso ya iniciado en otros países. Y no sólo eso sino que también se indica que la posición de España en el orden mundial depende de la acertada resolución de estos nuevos retos de la técnica. Sea como fuere, los millones de personas conectadas a la Red justifican por sí solo la insoslayable necesidad de proceder a un análisis multidisciplinar de la misma.

La vida de la Comisión está jalonada por veintiuna sesiones y cincuenta comparecencias en las que intervinieron un importante elenco de especialistas en la materia objeto de sus trabajos. El Informe emitido por la misma fue aprobado por el pleno del Senado el 17 de diciembre de 1999 y publicado en el *Boletín Oficial de las Cortes Generales* en su núm. 812, el 27 de diciembre de 1999. En las conclusiones de dicho Informe se reconoce que «las nuevas tecnologías de la información (...) transforman de forma sustancial la economía, las relaciones humanas, la cultura y la política en nuestra sociedad».

§ 3. Al margen de los objetivos de la Comisión *ad intra* podemos señalar que también se han perseguido unas finalidades paralelas al estudio de

los problemas jurídicos, políticos y sociales que plantean las redes de información. Nos referimos al deseo de proyectar a toda la Cámara la ineluctable necesidad de posicionarse en la vanguardia de las nuevas tecnologías (que, por otra parte, nosotros preferimos denominar nuevas técnicas). Para ello había que modificar la actitud del Senado e involucrarse en iniciativas innovadoras.

Con el deseo de corroborar el éxito logrado en esta dimensión *ad extra* se cita la creación de la página web de la Comisión, concebida técnicamente como un «link» o hipervínculo dentro de la página del Senado (http://www.senado.es). En el Informe se valora esta experiencia de manera extraordinariamente positiva llegándose a señalar que supuso la introducción del primer supuesto de Parlamento electrónico. Los riesgos que un Parlamento electrónico implica (basta sólo pensar, a nuestro entender, en la saturación o colapso del mismo, producto de una suerte de democracia directa de la era digital) son menores, a juicio de la Comisión, que los que «se podrían derivar del hecho de que el Senado permanezca al margen de la evolución, por no decir "revolución" tecnológica y social, que hoy en día se está produciendo y de la que todos podemos ser protagonistas». Esta iniciativa es vista como beneficiosa para el sistema democrático en su conjunto y para una mejor construcción del siempre complejo proceso de la toma de decisiones.

La búsqueda de nuevas formas de participación y el intento de acercamiento a la opinión pública llevó a la creación de un apartado en la página web de la Comisión denominado «Foro Público», en el que cualquier persona desde cualquier lugar del planeta pudo manifestar sus opiniones. Ello se tradujo en la posibilidad de realizar un segundo debate que complementase al que tenía lugar en la Comisión. Surgen, así, dos espacios de discusión, uno real y otro virtual, lo que sin duda ha sido un hito histórico en el funcionamiento parlamentario español. La operatividad del segundo creemos que aún está por demostrar, sobre todo si se consultan las opiniones vertidas por la mayoría de los ciudadanos que plasmaron sus ideas en el aludido «Foro Público». Quizá en el futuro la participación directa a través de la Red cambie en parte los actuales esquemas de democracia representativa, pero en la actualidad ello no parece todavía en modo alguno viable.

III. Derecho a la intimidad e informática

§ 4. La Constitución española de 1978 recoge en su art. 18, entre otras cosas, el derecho a la intimidad, la inviolabilidad del domicilio, el secreto

de las comunicaciones y establece 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 (3). Esta última previsión 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» (4), sino también como el reconocimiento de un nuevo derecho fundamental que va más allá de un mero mecanismo de garantía al verse la intimidad desbordada por el bien jurídico a proteger en este último caso (la genérica defensa de la personalidad) (5). La ley a la que se remite el artículo es en la actualidad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que deroga la anterior Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Además, podemos citar el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (modificado a su vez por el Real Decreto 156/1996, de 2 de febrero) y el Real Decreto 1332/1994, de 20 de junio, por el se desarrollaban ciertos aspectos de la ya derogada Ley Orgánica 5/1992.

Esta preocupación es compartida en otros muchos instrumentos normativos de ámbitos y latitudes muy diferentes. Así, en nuestro continente hay que nombrar el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, y las Directivas 95/46 sobre Protección de la Intimidad de los Ciudadanos y la 97/66 sobre el Tratamientos de Datos Personales y la Protección de la Intimidad en el Sector de las Telecomunicaciones. Para el estudio de

---

(3) La regulación constitucional ha sido objeto de diversas críticas, como las de PÉREZ LUÑO, 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 art. 105 b) de la Constitución, antes bien genera un «defecto sistemático» (PÉREZ LUÑO, Antonio Enrique, *Derechos humanos, Estado de Derecho y Constitución*, Tecnos, 6ª ed., Madrid, 1999, págs. 338 y sigs.).

(4) ÁLVAREZ-CIENFUEGOS SUÁREZ, José María, *La defensa de la intimidad..., op. cit.*, pág. 15.

(5) En este último sentido, por ejemplo, FERNÁNDEZ SEGADO, Francisco, «El régimen jurídico del tratamiento automatizado de los datos de carácter personal en España», *Derecho-PUC*, núm. 51, diciembre 1997, pág. 19; o LUCAS MURILLO DE LA CUEVA, Pablo, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, pág. 120. Una línea similar de interpretación se desprende de la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, fundamento jurídico 6. En otro sentido, puede verse RUIZ MIGUEL, Carlos, *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995, págs. 94 y sigs.

la aplicación de estas directivas el llamado Grupo del Artículo 29 creó 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 pretenden establecer unas pautas que se deberían seguir de forma escrupulosa en la interceptación legal de las telecomunicaciones. Más recientemente podemos citar la Decisión 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, que aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet.

La Comisión Especial sobre Redes Informáticas, en la cuarta de sus conclusiones, afirma que «el ordenador personal y el domicilio electrónico son inviolables». Y 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» (*Boletín Oficial de las Cortes Generales*, núm. 812, 27 de diciembre de 1999, pág. 46). Como se ve, se están parafraseando los párrafos segundo y tercero del art. 18 de la Constitución para equiparar al domicilio de este último artículo el domicilio electrónico y el ordenador personal, y para incluir en las comunicaciones las de tipo electrónico. Esta última idea ya estaba clara pues la redacción del art. 18.3 de la 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. Partiendo de la idea de intimidad se recogen, por lo 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» (6), o sea,

---

(6) STC, de 13 de enero de 1998, fundamento jurídico 11. Los textos normativos no suelen definir la idea de intimidad sino que se limitan a recoger los casos que agreden a la misma. La doctrina distingue de la intimidad la noción de privacidad (derivada directamente de la inglés «privacy») concibiendo ésta como más amplia que aquélla al aludir a datos no íntimos pero que la persona quiere que no sean difundidos. 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 «Geheimpsphäre» y «Sozialsphäre»). Nosotros no vamos a entrar en esta distinción por considerar que la finali-

un reducto personal y privado frente a posibles agresiones exteriores y frente al conocimiento de los demás, tiene unas particulares exigencias cuando entran en liza la informática y las redes, llegando incluso a propiciar, según se indicó más arriba, la configuración de un nuevo derecho fundamental. Como indica PÉREZ LUÑO, el respeto a la intimidad se ha convertido en «una de las exigencias más acuciantes que hoy gravita sobre la sociedad tecnológicamente avanzada» (7). No sólo debe ser vista desde una óptica negativa, como posibilidad de reaccionar frente a una invasión, sino también desde una dimensión positiva que permite controlar las informaciones que atañen a un sujeto. Por un lado, entre otras cosas, 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*). Por otro, garantiza el no acceso al 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.

Los avances técnicos han dado lugar a nuevas formas de agresión de la intimidad y de 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, la elaboración de perfiles del navegante (construidos en torno a su vida privada) con fines publicitarios u otros menos confesables, la simple acumulación o registro de datos, la interceptación de mensajes de correo electrónico, la suplantación de personalidad, el hostigamiento electrónico, el uso indebido de directorios de correo electrónico o listas de usuarios, y la transferencia de datos personales. Los perfiles de esas agresiones resultan en algún caso confusos, superponiéndose y conectándose. A veces el software que se emplea en tales actividades se crea de forma específica para ello. Estas agresiones, algunas de ellas fáciles de

---

dad de este trabajo así lo aconseja. En las comparecencias ante la Comisión cuya labor comentamos se produjeron algunas reflexiones, muy superficiales, en torno a la diferencia entre intimidad y privacidad (por ejemplo, el 29 de abril de 1999, en las págs. 17 y sigs. del *Diario de Sesiones del Senado* de dicho día).

(7) PÉREZ LUÑO, Antonio Enrique, *Derechos humanos...* , *op. cit*, pág. 317. Más adelante reitera esta 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» (págs. 345-346).

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 la globalización de la información. El anonimato que es posible buscar en Internet, al que coadyuva las dimensiones de la Red, favorece que se produzcan vulneraciones de los derechos que conciernen a la vida privada. Esta situación ha tratado de ser retratada 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, afirmación citada por el Consejero Delegado de Prisa, José Luis CEBRIÁN ECHARRI, en su comparecencia ante la Comisión el 20 de octubre de 1998. 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 que el desarrollo hace que «cada día sea más difícil conservar intacto el ámbito de la propia vida privada» (8).

El mundo de Internet incluso ha creado una jerga particular. Así, las vulneraciones que se producen a través de Internet del derecho a la intimidad han llevado a la aparición de palabras y expresiones para denominar, por ejemplo, a las personas que las llevan a cabo. De este modo, 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 un ordenador o a una red sin tener autorización para ello) y de *phone phreaker* (pirata especializado en compañías telefónicas) (9). Frente a sus intenciones se interponen «cortafuegos», o sea, mecanismos de seguridad que protegen los ficheros de ciertos servidores para impedir la incursión de personas no autorizadas. Los programas que se usan para atacar a los ordenadores se denominan «troyanos» (tratan de averiguar con engaños la contraseña de acceso), y los que recogen la información una

(8) FERNÁNDEZ ESTEBAN, María Luisa, *Nuevas tecnologías, Internet y derechos fundamentales*, McGraw-Hill, Madrid, 1998, pág. 137.

(9) Los tribunales españoles 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 fenómeno *hacking* como un intrusismo informático o interferencia o acceso no autorizado a un sistema informático.

vez dentro se les llama «gusanos», que son programas que una vez introducidos en un sistema son capaces de reproducrise por sí solos. A su vez, un «sniffer» es un programa rastreador en busca de usuarios y contraseñas. Igualmente, se habla de galleta o «cookie» para aludir a los dispositivos que se colocan dentro de los ordenadores y que recaban datos del mismo y de su usuario sin que éste detecte que está siendo inspeccionado. Una «cookie» es un fichero, no un programa, que llega al ordenador al consultar una página web y que en principio no tienen malas intenciones sino que son cooperativas al facilitar la navegación, aunque el uso que a veces se hace de ellas resulta, como indicaremos más abajo, inadmisible.

IV. Criptografía e interceptación

§ 5. Como defensa frente a los peligros que suponen para la intimidad las redes informáticas la Comisión aboga por la encriptación, que es un proceso de protección de datos mediante un cifrado de los mismos que evita una manipulación no deseada. No se entra en excesivos detalles a pesar de la relevancia de la cuestión pues, 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 encriptación se encuentra expresamente admitida en el art. 52 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones. La Unión Europea también reconoce la utilidad de las técnicas criptográficas habiendo adoptado su Comisión 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».

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. El emisor aplicaba esta clave para cifrar el mensaje, que a continuación era enviado al receptor, el cual 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.

En la actualidad se usa el llamado sistema de clave pública, en el cual existen dos claves, una pública y otra privada, que sirven tanto para codifi-

car como para decodificar, pero no por sí solas sino que son necesarias las dos puesto que si una codifica la otra es imprescindible para decodificar el mensaje. La complementariedad de ambas se basa en una fórmula compleja que impide que del conocimiento de la clave pública se llegue a la clave privada. 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. 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 utilizará la 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 las cosas, el sistema de la doble clave no necesita un canal seguro para enviar la información puesto que si se intercepta el descifrado resulta extremadamente difícil, llegando a supuestos en los que en la práctica es inviable dado el tiempo que llevaría. En efecto, 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 NSA norteamericana. No obstante, es realmente posible descubrirla si se tienen medios, capacidad y, sobre todo, tiempo para ello (años quizá). Hace un par de 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 dicho sistema se suela utilizar para enviar una de las claves tradicionales, procediéndose, a continuación, al envío de la información cifrada con esta clave tradicional.

La encriptación puede originar un choque de intereses entre la garantía de la privacidad y la seguridad pública, pues podría servir para tapar activi-

dades delictivas y/o contrarias a los intereses del Estado. Por ello, y como se hicieron eco algunos de los comparecientes ante la Comisión, en diversos países 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 en un lugar custodiado por un ente público. Estas propuestas 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, 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 (10), que no parece ser la que prima ahora en España pues el art. 52.3 de la ya citada Ley General de Telecomunicaciones establece que los operadores de redes que «utilicen cualquier procedimiento de cifrado deberán facilitar a la Administración General del Estado, sin coste alguno para ésta y a los efectos de la oportuna inspección los aparatos decodificadores que empleen», previsión que estimamos de dudosa constitucionalidad ya que puede dar lugar a un intervención de las comunicaciones contraria a las previsiones de la Carta Magna en tanto en cuanto no se exige intervención judicial.

§ 6. La Comisión no se planteó desde el punto de vista de la intimidad otros problemas de importancia que afectan a dicho derecho en Internet y que también se conectan con la encriptación. Aludimos a cuestiones tales como la firma digital, que sólo fue tratada desde el punto de vista del co-

(10) Uno de los comparecientes, David CASACUBERTA SEVILLA, presidente de la ONG «Fronteras Electrónicas España», criticó una hipotética ley que contenga exigencias como las de la existencia de bases de claves privadas («mandatary key recovery system»), pues lo que se hace es «torpedear» la propia ley al conseguir que «la criptografía deje de ser un sistema que me garantice la inviolabilidad de la correspondencia». Si la criptografía se hace insegura —prosigue— deja de tener sentido (*Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 308, Comisión Especial sobre Redes Informáticas, 16 de junio de 1998, pág. 19). Los sistemas de registro de las claves privadas no acabarán con la criminalidad pues ésta seguirá utilizando claves que nunca registrará (*ibidem*, pág. 24).

mercio electrónico, al margen de alguna alusión genérica, y el certificado digital. Con la firma digital se persigue garantizar el contenido de un mensaje en el sentido de que el receptor sepa que el mensaje no ha sido alterado en la Red, es decir, asegurar su integridad. Para realizar una firma digital se aplica al resumen del contenido del documento o *hash* (una especie de «extracto digital» que se hace derivar del mensaje, del que se extrae por un algoritmo) la clave privada del emisor surgiendo, así, 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 *hash*, tras lo cual comprobará si dicho *hash* se deriva realmente del mensaje transmitido. Si así es, el mensaje será el que en verdad ha enviado el emisor. Si el mensaje se hubiera alterado en el camino el *hash* no se corresponderá con el 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 (11). Con el certificado digital, en cambio, lo que se pretende es garantizar la identidad del origen, es decir, la autenticidad de los agentes implicados. Con él se sabrá quien es realmente el que hace la comunicación. Para obtener un certificado digital hay que acudir a una autoridad certificadora (por ejemplo, la Fábrica Nacional de Moneda y Timbre, en virtud de la Ley de Medidas Fiscales, Administrativas y del Orden Social de 30 de diciembre de 1997) que, en función de las características y referencias del sujeto que quiere obtener el certificado digital, le asigna un número. A continuación, esa autoridad certificadora codifica este número con su clave privada, obteniéndose, de este modo, el certificado digital del sujeto que lo ha solicitado. En las comunicaciones este sujeto enviará dicho certificado digital. El destinatario utiliza la clave pública de la autoridad certificadora para decodificar el certificado y obtener los rasgos del emisor, que permiten corroborar que la comunicación procedía en realidad de ese determinado emisor.

V. Otras agresiones

§ 7. Las agresiones a la intimidad distintas de la interceptación de mensajes tienen, a veces, más difícil respuesta. Así, ante la elaboración de per-

(11) 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.

files de los navegantes un usuario «medio», o sea, no experto, poco puede hacer salvo acudir a un ordenador diferente al suyo. Un gran número de empresas tiene sumo interés en conocer los hábitos de navegación del internauta. La navegación por la Red origina un rastro perfectamente detectable, rastro que se traduce en ciertos datos que sirven de base para la construcción del perfil. A veces los datos que se extraen de los ordenadores personales son necesarios, como los datos técnicos que un suministrador obtiene del ordenador 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. Teniendo este dato se tiene localizado al usuario que será detectado cuando entre en una página web determinada, aunque la cosa se complica si la dirección IP que se usa es móvil y no fija. 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. 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. Incluso hay sitios cuya publicidad correrá a cargo de centrales interactivas que con bastante probabilidad realizarán procesos de agregación de datos de los usuarios. 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. El internauta, de esta forma, 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).

Por su parte, las entradas al disco duro se llevan a cabo con programas denominados en la jerga al uso «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 en una escala de gravedad a pesar del escaso eco que tuvieron en la Comisión, son muchas las variables que influyen facilitándolas o entorpeciéndolas. Los medios de prevención pueden ser contraseñas y códigos de acceso cuya eficacia de-

penderá 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. 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 ó 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 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. La cuestión surgió sólo colateralmente en el seno de algún debate con los comparecientes ante la Comisión (12).

La Recomendación 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. De igual modo, la Comisión señala en su Informe que de las garantías de seguridad que ofrezcan las entidades presentes en la Red «dependerá en gran parte la fiabilidad en las relaciones que implican intercambio de datos» (*Boletín Oficial de las Cortes Generales*, núm. 812, 27 de diciembre de 1999, pág. 36).

En la Comisión se puso de manifiesto la creciente importancia que en España tiene el acceso no autorizado a sistemas informáticos, la alteración de los mismos, el apoderamiento de ficheros, la interceptación ilegal de correo electrónico y el intrusismo informático, que pueden entrar dentro del

(12) Por ejemplo, el 16 de junio de 1998, con David CASACUBERTA, en la comparecencia citada más arriba (*Diario de Sesiones del Senado*, núm. 308, pág. 23).

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, manifestándose esta tendencia también en actividades terroristas (13).

Asimismo, en las comparecencias ante la Comisión se dejó constancia de los problemas que genera 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 (14). También se mostró preocupación por las «cookies» que las páginas web a las que se accede o, mejor dicho, el servidor del sitio web al que se accede coloca en el ordenador del usuario, haciendo que dicho usuario esté identificado e, incluso, que se destruya o controle la información que el usuario maneja en ese momento. Ante ello el senador LAVILLA MARTÍNEZ plantea la siguiente reflexión: el usuario «sólo ha accedido a una información que ha querido incorporar a su ordenador personal, y ese acceso ha permitido a una determinada empresa controlar datos de tipo personal» (15).

En cambio, la venta de datos personales entre empresas sin autorización de los afectados no fue objeto de reflexión en la Comisión. Este es otro problema grave que ocurre con demasiada habitualidad (la empresas norteamericanas 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.

VI. El reto de los poderes públicos *vs.* retirada del Derecho

§ 8. Los poderes públicos, como consecuencia de la cualidad de garantes que se les predica, deben llevar a cabo campañas de información para que los ciudadanos conozcan las opciones técnicas de seguridad informáti-

---

(13) Así quedó reflejado con la comparecencia de dos expertos de las Fuerzas y Cuerpos de Seguridad del Estado el 30 de septiembre de 1999 (*Diario de Sesiones del Senado*, VI Legislatura, Comisiones, n.º 488, Comisión Especial sobre Redes Informáticas).

(14) En estos términos se expresó el Director de la Agencia de Protección de Datos en su comparecencia el 29 de abril de 1999 (*Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 428, Comisión Especial sobre Redes Informáticas, pág. 16).

(15) *Ibidem*.

ca y promover que los productos de hardware y de software para Internet faciliten a los usuarios, como señala la Comisión en su Informe, «información sobre los datos que pretenden recoger, almacenar o transmitir y con qué finalidad lo harían». Esto sería un paso importante habida cuenta la parcial analfabetización digital todavía existente en España, aunque inicialmente poco podría hacerse frente a ciertas agresiones, como los intentos camuflados de acceso no consentido a los datos personales y de interceptación no detectada de las comunicaciones. En un momento posterior, cuando la concienciación de los usuarios ya los haya convertido en precavidos, la labor de los agresores de la intimidad se vería obstaculizada hasta el punto de ser desaconsejable. No obstante, estas afirmaciones hay que recubrirlas con dosis de relatividad dadas las diversas variables que intervienen en esta cuestión, teniendo en cuenta, sobre todo, que los hipotéticos avances futuros en el campo de la informática y de la matemática, ahora desconocidos, podrían convertir en mucho más vulnerables las medidas de protección existentes. En España ya se han publicado en fechas recientes estudios que revelan la inseguridad de un altísimo porcentaje de páginas dedicadas, por ejemplo, al comercio electrónico.

En este orden de cosas, sería conveniente arrojar luz sobre los mecanismos que estarían autorizados para proceder a la interceptación y recogida de comunicaciones y datos personales que, según los senadores, y evidentemente, «sólo podrá hacerse con autorización judicial», cosa que no siempre sucede en el Derecho Comparado y que incluso, como ya vimos más arriba, nuestra Ley General de Telecomunicaciones parece obviar. La interpretación de los medios lícitos para tales operaciones y de los supuestos en los que procedería debe ser restrictiva como exigencia del principio de mayor valor de los derechos.

§ 9. Ante la imposibilidad de ejercer un eficaz control de Internet la Comisión parece, por un lado, preconizar una huida del Derecho al postular la necesidad de elaborar códigos éticos, y, por otro, estimular formas de autocontrol como resultado de la aplicación del principio de la autonomía de la voluntad de los particulares. Ambas ideas están muy conectadas pues una asociación de particulares que quiera establecer sus propias normas debe basarse en gran parte en lo ético ya que carecerá del aparato coactivo estatal para imponer por la fuerza dicha normativa (16). Se alude, para justificar

(16) ESCOBAR DE LA SERNA opina que toda la actividad de Internet se materializa en el concepto ético, que Richard MASON «sintetizó con el acrónimo PAPA» —*privacy, accu-*

esta opción, a los problemas de competencia que acarrea la ausencia de territorialidad, lo cual es, por otra parte, una simplificación de todo punto exagerada, que habrá que enfrentar, como también apunta la propia Comisión, con una armonización de la legislación internacional. En cambio, en otros momentos la propia Comisión concluye que es obligación de las autoridades garantizar el acceso a Internet, para lo cual es preciso conjugar varios factores, entre los que está la regulación de la Red.

Como acabamos de decir, lo que se aconseja en unas ocasiones es que las autoridades públicas se retiren (17). Ello contrasta con lo se percibe en algunas ramas del Derecho, como el Derecho Penal o el Derecho Tributario, en las que se buscan nuevas soluciones para mantener bajo control el fenómeno de Internet. Así, en el Derecho Tributario han aparecido propuestas como la creación de un tributo específico (el «bit tax»), que se aplicaría «en función del tamaño (número de bits) de los ficheros descargados desde la red, con objeto, entre otras cosas, de compensar la pérdida de recaudación que, tanto desde el punto de vista de la imposición sobre la renta como del IVA, puede suponer un comercio virtual con evidentes dificultades para un control fiscal efectivo» (18). Igualmente, en el Derecho Tributario se ha debatido con intensidad la solución a la falta de eficacia en el campo de las redes informáticas de los criterios tradicionales de sujeción a un determinado poder tributario, es decir, del principio de territorialidad y del principio de nacionalidad. Por su parte, en el Derecho Penal ya existen diversas referencias y previsiones que afectan directamente a la Red y tipos penales en los que consta la utilización de una serie de medios informáticos (por ejemplo, el descubrimiento y revelación de secretos del art. 197 del Código Penal de 1995 habla, como medio para descubrir secretos o vulnerar la intimidad, del correo electrónico, que también debe ser tenido en cuenta en el descubrimiento de secretos de empresa del art. 278).

---

racy, property, accessibility— (ESCOBAR DE LA SERNA, Luis, «Las libertades informativas en la nueva sociedad de la información», en el libro por él editado *Sociedad, Información y Constitución*, *op. cit.*, pág. 85).

(17) Desde la «Federal Communication Commision» de los Estados Unidos se trata de encontrar nuevos modelos que permitan evitar la regulación, al tiempo que sirvan para la mejora de la competencia y de la universalización del servicio. Este órgano ha propiciado una libertad en Internet desligada de requisitos y regulaciones.

(18) FALCÓN Y TELLA, Ramón, en el editorial del núm. 10 de 1998 de *Quincena Fiscal*, pág. 5. La dificultad de implantar un impuesto así ha llevado a que se busquen vías alternativas de sujeción, pero no a eximir de gravamen.

Desde unos postulados tradicionales, y un tanto simplistas, no semeja muy afortunada la velada recomendación de la Comisión de dejar el Derecho al margen. En efecto, desde un punto de vista general puede afirmarse que el Derecho, fenómeno que regula la sociedad, debe abordar aquello que merece ser regulado, dejando sólo de lado lo que por carecer de importancia no resulta necesario prever. Sin duda, Internet no pertenece a la categoría de cuestiones irrelevantes que no es preciso abordar, sino que la trascendencia que atesora exige que lo jurídico le preste especial atención. Las dificultades técnicas para aproximarse a la red de redes no pueden ser una eximente para soslayar la necesidad de regularla. Otra cosa es que una vez realizada dicha regulación se vea que lo más operativo es no introducir *ius cogens*, o sea, normas de cumplimiento obligatorio sino hacer prevalecer los acuerdos de los particulares sobre la previsión normativa, que en todo caso debe existir. Sin embargo, en esta línea argumentativa puede no ser conveniente introducir normas de Derecho voluntario dada la relevancia del fenómeno de Internet y el interés general que se puede predicar que ostenta. Un interés general que puede llegar a conectarse a la idea de servicio público, que es utilizada por la Comisión unas veces de una forma técnico-jurídica y otras, la mayoría, de un modo más genérico e impreciso (19).

No obstante, partir en esta cuestión de otros postulados da lugar a un razonamiento diferente. El fenómeno de las telecomunicaciones puede ser analizado en términos de libertad de expresión y comunicación, lo que puede chocar con la idea de servicio público. Ésta lleva a la titularidad pública del servicio y a la concesión para que un particular lo ejerza, mientras que la presencia en la materia de derechos fundamentales impediría tal titularidad pública y desembocaría, en todo caso, en una autorización, que es compatible con un previo derecho subjetivo del particular. La situación inicial del particular ante la actividad sería la de libertad (20). Ante ello, la opción de retirar el Derecho no resultaría incorrecta.

---

(19) Es el caso, creemos, de lo que se dice en las conclusiones del Informe: «Internet debe convertirse en un servicio público universal» (*Boletín Oficial de las Cortes Generales*, núm. 812, 27 de diciembre de 1999, pág. 45). En cambio, en la página siguiente sí parece emplearse la expresión en un sentido técnico-jurídico.

(20) Esta problemática se planteó, por ejemplo, en la jurisprudencia del Tribunal Constitucional de 1994 sobre la televisión por cable.

En realidad, razonar en términos de servicio público (21) resulta una agresión a lógica por las características de Internet, que dejan en lo absurdo la *publicatio* de una actividad virtual y sin fronteras (otra cosa es, por ejemplo, la instalación de la RDSI). La regulación de la Red no debe buscar el control sino la garantía del desarrollo de la actividad en términos igualitarios, de eficacia y de universalidad del acceso. Asimismo, debe ofrecer mecanismos reparadores ante las vulneraciones de los derechos de los particulares, que previamente han sido educados en las características del medio para que sepan protegerse de eventuales intromisiones. Aunque resulte innecesario recordarlo, es preciso conjugar, por un lado, libertad de expresión y comunicación y, por otro, derecho al honor y a la intimidad. El carácter preferente de las libertades indicadas, en tanto que son medio para la formación de una opinión pública libre, debe llevar a subrayar el aspecto de garantía de la actividad antes que el de control. Pero llevar a cabo esta función de garantía no es abstenerse sino, entre otras cosas, efectuar una regulación encaminada a cumplir con tal fin. Por lo tanto, la retirada del Derecho resulta un error en esta materia.

La aproximación al tema de la regulación de Internet es, en el fondo, harta compleja. La cuestión quizá esté, como afirma ESCOBAR DE LA SERNA, no tanto en «la necesidad o, al menos, la conveniencia de su regulación, sino en el cómo» (22). En efecto, los esquemas aplicables a los medios de comunicación tradicionales no son muy útiles pues éstos responden a unos parámetros muy distintos. En Internet se produce una confusión entre medios de comunicación de masas y medios de comunicación individual. No hay, como era lo tradicional en un medio de comunicación de masas, una comunicación unidireccional entre un centro emisor activo y un gran número de receptores pasivos sino que la interacción recíproca difumina los conceptos de emisor y de receptor y provoca una comunicación multidireccional. Ello hace que las reflexiones de mayor intervención (en la televisión o la radio, por ejemplo) o de intervención mucho menor (en la prensa escrita, *v. gr.*) haya que reconstruirlas, cosa que ahora no nos atañe. Sea como fuere, parece que la regulación debe ser tanto de índole nacional

(21) El Presidente del Instituto Catalán de Tecnología, Joan MAJÓ CRUZATE, en su comparecencia ante la Comisión abogó por que rigiera el principio del servicio público «como ocurrió con la implantación de la telefonía y la televisión».

(22) ESCOBAR DE LA SERNA, Luis, «Las libertades informativas..., *op. cit.*, pág. 81.

como internacional, debiendo partir de la idea de libertad complementada por las de seguridad y responsabilidad.

VII. LAS COMPARECENCIAS

§ 10. En algunas de las comparecencias de expertos ante la Comisión, aparte de las ya citadas, se abordó de manera directa la cuestión de la intimidad. Así, Mario RUIZ TASCÓN, subdirector del diario «El Mundo» señaló los peligros de la monopolización de la Red para el derecho a la intimidad y la libertad de expresión, ante lo cual los poderes Legislativo y Judicial deben ser sensibles para reaccionar. De igual forma, consideró que debería recomendarse a quienes reclaman datos sobre los clientes que lo hagan saber y especifiquen, antes de recogerlos, el uso que van a hacer de ellos. Además, abogó por que la Agencia de Protección de Datos extienda su vigilancia a Internet y que se potencie la criptografía como derecho básico del ciudadano (23). Precisamente, para otro periodista que acudió a la Comisión, esta vez de «Cinco Días», José CERVERA GARCÍA, la encriptación en las transacciones lleva a una colisión con «la necesidad que pueden tener en algunos momentos las fuerzas de seguridad del Estado de leer un correo electrónico», lo que origina el problema político de «decidir hasta qué punto vamos a proteger el comercio electrónico y hasta qué punto vamos a proteger la seguridad del Estado» (24). Por su parte, David CASACUBERTA, presidente de la ONG «Fronteras Electrónicas España», también abordó, aparte de los sistemas de filtrado y bloqueo, la cuestión de la criptografía para señalar el peligro que existe dada la falta de garantías de seguridad absoluta. Igualmente, entiende (como ya señalamos en la nota diez de este trabajo) que las claves criptográficas no han de ser susceptibles de control por parte de la Administración sino que cada usuario debe poder decidir sobre su propia clave.

María Luisa FERNÁNDEZ ESTEBAN, profesora de Derecho Constitucional de la Universidad Autónoma de Madrid, analizó expresamente el

---

(23) «No debe sucedernos como en Francia, donde la prohibición estatal del uso de la criptografía está retrasando el desarrollo del comercio electrónico y tecnológico de muchas de sus empresas» (*Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 305, Comisión Especial sobre Redes Informáticas, 15 de junio de 1998, pág. 3).

(24) *Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 318, Comisión Especial sobre Redes Informáticas, 30 de junio de 1998, pág. 5.

impacto de Internet en el derecho a la intimidad, al margen de reflexionar sobre la libertad de expresión y los nuevos conceptos a ella ligados (listas blancas, listas negras, etiquetado de páginas, filtros, programa «Prudence»). Los dos peligros fundamentales que, según la compareciente, se detectan para la intimidad son la difusión mundial de los datos personales y la elaboración de perfiles de los usuarios de Internet según las páginas visitadas. El acopio de datos permite la elaboración de perfiles cada vez más precisos de las personas. Este acopio se hace por medio de las ya comentadas «cookies» o del correo electrónico en tanto en cuanto el particular accede a ciertos boletines de información o a grupos de discusión. Y de nuevo se apela a la criptografía como solución para ofrecer confidencialidad, integridad y autenticidad en la información transmitida, haciéndose eco, al mismo tiempo, de los choques que ello provoca con la necesidad de proteger la seguridad nacional. «La confidencialidad es víctima de su propio éxito» (25).

A su vez, Tomás DELCLÒS i JUANOLA, periodista del diario «El País», abogó por la primacía de la garantía de la privacidad sobre la seguridad pública en Internet, alegando para ello, en la línea de David CASCUBERTA, que «el criminal que quiera utilizar Internet, obviamente no va a acudir a los sistemas criptográficos más popularizados, sino que va a generar su propio mecanismo de conexión bilateral», no pudiendo la ley «resolver esta argucia». Es la privacidad la que está en una situación de más peligro en Internet que la seguridad pública (26).

Finalmente, el director de la Agencia de Protección de Datos, Juan Manuel FERNÁNDEZ LÓPEZ, recordó los principios que rigen la recogida de datos en la normativa española y europea, entre los que se halla la calidad de los datos (adecuados, pertinentes, no excesivos, usados para la finalidad para la que se recabaron, cancelándose cuando dejen de ser necesarios), el derecho a la información en la recogida de datos (aquellos a los que se les soliciten datos deberán ser informados de la existencia de ficheros, del carácter obligatorio o facultativo de sus respuestas, y de la posibilidad del ejercicio de los derechos de acceso, rectificación y cancelación de los mis-

---

(25) *Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 308, Comisión Especial sobre Redes Informáticas, 16 de junio de 1998, págs. 4 y 5. La compareciente aludió a algoritmos de 64 dígitos como extremadamente seguros en la criptografía. Hoy, como ya indicamos más arriba, se recomiendan más de cien dígitos.

(26) *Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 305, Comisión Especial sobre Redes Informáticas, 15 de junio de 1998, pág. 15.

mos) y el consentimiento del afectado (no se pueden recoger datos sin dicho consentimiento salvo excepciones, excepciones que deben girar en torno a una relación negocial o al supuesto de que los datos se recojan de fuentes accesibles al público). Igualmente señaló con rotundidad que no se puede permitir «que no se encuentren soluciones satisfactorias para los problemas jurídicos nacidos de la falta de adecuación del Derecho a las normas de comportamiento de la sociedad de la información» (27).

VIII. Reflexiones finales

§ 11. Quizá los objetivos que se plantearon en la Comisión fueron demasiado amplios (o quizá la aspiración de conseguir conclusiones de consenso llevó a un exceso de generalidad), lo que ha dado lugar a que su labor no haya sido exhaustiva en casi ninguno de los puntos abordados. Se ha hecho un recorrido por una gran variedad de cuestiones que plantea Internet, desde aproximaciones jurídicas a técnico-informáticas pasando por reflexiones sociológicas, económicas y filosóficas. La conclusión de todo ello permite subrayar la enorme trascendencia que el fenómeno de Internet tiene y, sobre todo, va a tener en el futuro, y mostrar una serie de pautas generales que deben tenerse en cuenta, pautas, por otra parte, en ningún modo novedosas e, incluso, ya asentadas en determinados círculos intelectuales. Se ha perdido la oportunidad de profundizar en algunas de las cuestiones polémicas que en la actualidad aún están construyéndose y de marcar una pauta clara que sirviese de recomendación para el proceder de los múltiples agentes implicados en el fenómeno. Los principios que se extraen de sus trabajos son, al igual que en los documentos que prepara la Unión Europea, programáticos y políticos, entre los que aparece con nitidez la necesidad de garantizar el acceso de todos los ciudadanos a la Red, que se logrará con el concurso de variables económicas, culturales, técnicas, sociales y jurídicas. Los poderes públicos están llamados a jugar un papel esencial en esta labor de universalización del acceso, que debe verse acompañada por dosis de calidad que jueguen a favor de la conectividad y de la capacidad de proceso (28).

---

(27) *Diario de Sesiones del Senado*, VI Legislatura, Comisiones, núm. 428, Comisión Especial sobre Redes Informáticas, 29 de abril de 1999, pág. 13.

(28) La Comisión, en las conclusiones de su Informe, califica la universalización del acceso como «una necesidad, un servicio y un derecho que los poderes públicos deben garantizar, auspiciar y proteger», por lo que es obligación del legislador español «diseñar los mecanismos para poner al servicio de la inmensa mayoría de los ciudadanos y ciudadanas las

La realidad actual nos ofrece una especial vulnerabilidad en Internet de la intimidad y de la vida privada, lo cual se conecta con el gran aumento de la inseguridad informática en la Red. En la práctica parece particularmente útil el propósito de fomentar la divulgación entre los usuarios y ciudadanos de las medidas de seguridad existentes para la protección de la intimidad. Serían medidas de precaución, «camuflaje» y encriptación que, dadas las dificultades para superarlas si están bien construidas, garantizarían una seguridad muy importante ante algunos de los tipos de ataques que sufre la intimidad. Tales campañas de divulgación hay que conectarlas con los encargos constitucionales de promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y de remoción de los obstáculos que impidan o dificulten su plenitud (art. 9.2 Const.), y con la búsqueda de la igualdad de oportunidades y de acceso a los bienes de la información (art. 19 de la Declaración Universal de Derechos Humanos). Hay que tratar no sólo que no exista una fractura social entre los que acceden a la información y los que no, procurando que éstos entren en el grupo de aquéllos, sino también que la capacidad de garantizar la intimidad no sea cosa de pocos. En este orden de cosas, la educación es un factor a tener muy en cuenta, educación que tiene que abarcar todas las edades en un proceso continuo de actualización, que, aunque a algunos les suene a utópico, hay que considerar posible si se construye con la corrección necesaria. De poco sirve contar con poderosos medios de protección si son infrautilizados por desconocimiento. Además, la adecuada percepción de los problemas señalados en este trabajo hará más eficaces los principios éticos que desde diversas instancias se quieren introducir en Internet (29).

No obstante, y a pesar de todo, hay que valorar positivamente el intento de la Cámara Alta española de acercarse al mundo sin fronteras de la realidad virtual de la Red en un alegato a favor de la modernidad y como ejemplo para que instituciones públicas y privadas se suban al furioso corcel del avance técnico. Ello no es, ni mucho menos, sinónimo de progreso pero sí un elemento imprescindible para afrontar con garantía de éxito la marcha a

---

ventajas, los avances y los progresos que las nuevas tecnologías de la información ofrecen» (*Boletín Oficial de las Cortes Generales*, núm. 812, 27 de diciembre de 1999, págs. 45 y 46).

(29) España parece haber sido el primer país de la Unión Europea que elabora, en el seno de la Asociación Española de Comercio Electrónico, un código ético de protección de datos, en cuya difusión también están involucradas asociaciones de consumidores y la Asociación de Autocontrol de la Publicidad. La Agencia de Protección de Datos tiene especial interés en medidas de este tipo.

través del siglo veintiuno. En esta labor tampoco se pueden olvidar los peligros que se pueden detectar a día de hoy en Internet, algunos de los cuales citábamos en el primer párrafo de este trabajo. Unos peligros que pasaron en exceso desapercibidos por la Comisión (30).

En definitiva, y como hemos visto, los problemas actuales del fantástico fenómeno de Internet son muchos. Y no sólo eso sino que con toda seguridad seguirán apareciendo en el futuro nuevas y controvertidas cuestiones. Ante ello resulta necesario afrontar los desafiantes aspectos que presenta, no soslayarlos. La construcción de un sistema jurídico que dé eficaz y justa respuesta a la compleja realidad actual exige asumir nuevos retos. Uno de estos retos es, sin duda, Internet. El ordenamiento jurídico aún tiene mucho que decir, y de manera ineluctable en el terreno de los derechos fundamentales, clave de bóveda del Estado de Derecho.

(30) Algunos de los comparecientes llegaron a efectuar afirmaciones y propuestas que recalcan estos elementos negativos. Así, Pere BOTELLA, vicerrector de la Universitat Politécnica de Catalunya, propuso la creación de espacios de silencio didáctico frente al ruido de las aulas (*sic!*).