EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS E INTERNET EN LOS DERECHOS DEL ART. 18 DE LA CONSTITUCIÓN

Por Dña. MARÍA LUISA FERNÁNDEZ ESTEBAN
Área de Derecho Constitucional. Universidad Autónoma de Madrid

SUMARIO:

1. LA PROTECCIÓN CONSTITUCIONAL DE LA VIDA PRIVADA

1.1. Visión global de los derechos fundamentales del art. 18 de la Constitución

El art. 18 de la Constitución recoge *una pluralidad* de derechos con la siguiente dicción:

> «1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
>
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 4. la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.»

Del débil reconocimiento civil del honor, la intimidad y la propia imagen como derechos de la personalidad, la Constitución pasa a concebir estos derechos como fundamentales y, por tanto, pertenecientes a la persona en razón de su dignidad (art. 10 de la Constitución)[1]. La dignidad de la persona es inseparable de la definición del Estado como social y democrático de Derecho, presente en el art. 1.1 de la Constitución[2].

La formulación de estos derechos conjuntamente parece obedecer a una tendencia hoy dominante en el derecho comparado que tiende estudiar conjuntamente los distintos instrumentos de tutela jurídica de la vida privada. Así, la doctrina del Tribunal Constitucional ha tendido a mantener el carácter unitario del derecho al honor, a la intimidad y a la propia imagen, destinados a la salvaguardia de la vida privada. Aunque los derechos fundamentales del art. 18 mantienen su autonomía en virtud de su explícita mención en el art. 18, y porque así lo ha manifestado tanto la jurisprudencia ordinaria como constitucional, resulta interesante apreciarlos como instrumentos de tutela y protección de distintas facetas de un mismo bien jurídico: la vida privada de los individuos.

---

[1] Ll. de Carreras Serra, «Régimen Jurídico de la Información. Periodistas y Medios de Comunicación», *Ariel Derecho,* 1996, pág. 62.

[2] M. Carrillo, «Los Límites a la Libertad de Prensa en la Constitución Española de 1978», *P.P.U.*, 1987, pág. 36.

Una visión no fragmentada de los derechos del artículo 18 de la Constitución nos permite acoger las últimas tendencias de la jurisprudencia europea, que tienden a difuminar los límites entre estos derechos fundamentales, al enfrentarse a problemas de nueva factura que encuentran difícil acomodo en una concepción estanca y cerrada de los derechos fundamentales. Un ejemplo de esta tendencia es la famosa sentencia del tribunal de Derechos Humanos de Estrasburgo «López Ostra», de 9 de diciembre de 1994, en la que la entrada de humos y olores penetrantes en un domicilio se estimó contraria al derecho a la inviolabilidad del domicilio. Una visión más global de los derechos del art. 18 nos permite también ofrecer tutela constitucional frente a algunas acciones que permiten las nuevas tecnologías y frente a las que es difícil establecer cual es el derecho fundamental del art. 18 que está siendo vulnerado. El Tribunal constitucional en su sentencia S.T.C. 110/84, ponía de manifiesto que los distintos apartados del art. 18 de la Constitución:

> «...tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de la tecnología, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esta protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad, y del respeto a la correspondencia que es o puede ser medio de conocimiento de aspectos de vida privada.»

El desarrollo tecnológico de los sistemas de comunicación, la informática y las modernas técnicas de captación y grabación del sonido y la imagen hacen que cada día sea más difícil conservar intacto el ámbito de la propia vida privada, que no hace muchos años se salvaguardaba sólo con la protección del domicilio y la correspondencia.

Con las nuevas tecnologías e Internet, la protección de la vida privada no puede limitarse a la protección de la intimidad, sino que se trata de un concepto más amplio que necesita ser definido y protegido por la creciente difusión de la telemática[3]. La L.O.R.T.A.D. (Ley Orgánica 1/1992 Reguladora del tratamiento Automatizado de Datos de Carácter Personal) recoge en su exposición de motivos una distinción entre intimidad y vida privada que es reveladora:

> «el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad *(sic)* a una amenaza potencial antes desconocida. Nótese que se habla de privacidad y no de la intimidad. Aquella es más amplia que ésta, pues en tanto que la intimidad protege la esfera en que se desarrollan las facetas singularmente reservadas a la vida de la persona –el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo–, la privacidad constituye un conjunto más amplio,

[3] Ll. de Carreras, «Régimen Jurídico de la Información. Periodístas y Medios de Comunciación», *Ariel Derecho,* 1996, pág. 71.

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 tienen derecho a mantener reservada. Y si la intimidad en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del art. 18 de la Constitución y por las Leyes que lo desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo»[4].

1.2. La libertad informática del apartado 18.4 de la Constitución

La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (L.O.R.T.A.D.) Ley 5/92, junto con el Convenio de 28 de enero de 1981 sobre Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, da cuerpo al deber positivo a cargo de los poderes públicos de protección de la vida privada frente a la informática. La L.O.R.T.A.D. se aplica a los datos de carácter personal que figuren en ficheros públicos o privados, e incluso al uso no informatizado de esos datos.

La L.O.R.T.A.D. encuentra su fundamento constitucional en el art. 18.4 de la Constitución. El progreso tecnológico permite nuevas formas de control sobre la vida privada de los ciudadanos. La amenaza que supone la acumulación de datos sobre los individuos no sólo proviene del Estado, sino, especialmente de los grupos privados de amplia influencia social y económica que tienen acceso a los nuevos medios tecnológicos. Los grandes oligopolio periodísticos cuentan con medios eficaces para acceder a la esfera de lo privado de muchos ciudadanos. En este sentido, es cada vez más preocupante el creciente manejo de datos de los ciudadanos por parte de las empresas, los grandes intereses económicos, los bancos, etcétera.

La razón del mandato constitucional del art. 18.4 es el peligro real y efectivo que la acumulación informática de datos sobre las personas puede representar sobre la libertad y los derechos de los ciudadanos, en especial sobre la vida privada. La evolución rápida de las tecnologías y la manera en la que la informática se integra en la gestión de la administración o en el sector privado representa para los particulares una serie de desventajas.

Que los ficheros privados y públicos sean de libre acceso al público constituye para el ciudadano varios riesgos: de una parte, problemas de salvaguarda de la intimidad (datos sobre la salud, infracciones penales, periodos de inestabilidad laboral), de otra parte la creciente incertidumbre e inseguridad de no saber de qué manera la información concerniente un espacio de la vida privada va a ser utilizada. El legítimo interés constitucional de protección de la intimidad de las personas se limita en la medida en que la sociedad en general requiere del individuo ciertas informaciones. El conflicto se agrava en la medi-

[4] Citado por Ll. Carreras, *Ibidem*, pág. 82.

da en que crece el valor económico que poseen los datos sobre las personas. Compañías de seguros, bancos nacionales e internacionales, la empresa privada o la prensa solicitan continuamente datos sobre futuros o actuales clientes[5]. Por parte de la doctrina se ha propuesto incluso el reconocimiento de un nuevo derecho de propiedad sobre los datos de carácter personal, que se han convertido en una mercancía vital y de gran valor en la era del *direct-marketing*[6]. Lo que es claro es el carácter invasor de las tecnologías de la información, que se apoderan de la vida privada, la traducen en datos de fácil circulación y en una mercancía muy valiosa.

Este proceso imparable ha afectado también a la concepción de la vida privada en relación con la informática, que se configura no tanto como el «derecho a ser dejado en paz», sino, más bien como la posibilidad del ciudadano de controlar aquella información que se refiere a él[7].

La regulación de la protección de la vida privada frente a la informática debe ponderar dos tipos de intereses: por un lado la protección de la vida privada y por otro el interés general de la sociedad en la circulación de cierta información sobre el individuo. Para obtener un resultado ponderado no basta con individuar un «núcleo duro» de la vida privada al que asegurar la mayor tutela posible, y una franja de informaciones relevantes para la colectividad para la que se permite la publicidad y circulación: el punto de inflexión debe centrarse en el control, y no en el secreto[8].

2. VIDA PRIVADA, NUEVAS TECNOLOGÍAS E INTERNET: ¿LA DESNUDEZ DE LA INTIMIDAD?

En la comunicación electrónica, las fronteras entre lo público y lo privado tienden a difuminarse. Es cierto que la sociedad de masas permite el anonimato, pero la tecnología allana la vida privada. Nuestras inclinaciones políticas, las historias médicas, las finanzas, pueden encontrarse a disposición de muchos o casi cualquiera. La aldea global es esta desnudez de la «intimidad»[9].

Internet introduce una evidente amenaza para la protección de la vida privada ya que es posible la difusión de elementos relativos a la imagen y vida particular de los individuos a través de la Red. En 1996 tuvo lugar un caso paradigmático del desafío que entraña la globalización para los medios de protección de la intimidad y el honor que otorga el Derecho. F. Mitterrand, presidente de la República francesa durante muchos años, falleció durante las Navidades de 1995. Tras su muerte, el que había sido su médico particular durante décadas

[5] *Vid.*, P. van der Mensbrugghe, «Flujos Transfronterizos de Datos en la Directiva 95/46 de la Comunidades Europeas», *Actualidad Informática Aranzadi*, julio de 1996.

[6] S. Rodotà, «Tecnologie e Diritti», *Il Mulino*, 1994, pág. 13.

[7] *Ibidem*, pág. 102.

[8] *Ibidem*, pág. 33.

[9] V. Verdú, «La última revolución del siglo xx», *El País*, 22 de noviembre de 1994.

publicó un libro sobre los últimos momentos de su vida. El 18 de enero de 1996 el Tribunal de Grande Instancia de París ordenó el secuestro de la publicación a instancia de la familia de Mitterrand. El Tribunal estimó que el doctor Grubler había incurrido en violación del secreto profesional y había cometido una grave intrusión en la intimidad del expresidente[10].

Antes del secuestro ordenado por el Tribunal de Grande Instancia se habían vendido ya 40.000 copias del libro. Uno de los compradores que poseía un *cibercafé* introdujo en su servidor una copia del libro cuya venta había sido prohibida por el secuestro. El servidor estuvo colapsado durante varios días debido al intenso tráfico, pero además, el libro fue inmediatamente copiado o reflejado en servidores de organizaciones anticensura y pro-libertad de expresión de todo el mundo, y para finales de febrero ya había una copia en inglés disponible en numerosos servidores[11]. Este famoso caso pone de manifiesto dos aspectos preocupantes: en primer lugar la ineficacia de los instrumentos tradicionales otorgados por el Derecho, como es el secuestro judicial; en segundo lugar, el problema que genera la globalización de Internet que podríamos denominar *forum shopping*. Por lo que se refiere al primer aspecto, el secuestro garantiza la no difusión de obras en un mundo analógico, donde sólo se puede acceder al libro que se pretende secuestrar comprando la copia. De este modo, basta la prohibición para que no se difunda la obra. En Internet, la introducción de una sola copia en cualquier servidor del mundo puede suponer que, potencialmente, millones de personas tengan acceso a ella. Por lo que se refiere al segundo aspecto, este caso expone con toda su crudeza las limitaciones de los derechos nacionales en un mundo sin fronteras, como es el *ciberespacio*[12].

2.1. Protección de la vida privada y servicios interactivos

Los nuevos medios de comunicación interactivos, en particular Internet, se han convertido en un canal para el suministro de bienes o servicios a través de un intercambio de información cada vez más importante. Los datos ofrecidos por los interesados para obtener determinados servicios son tales, por cantidad y calidad, que permiten toda una serie de empleos secundarios, particularmente remunerativos, para los gestores de sistemas interactivos. Estos pueden elaborar perfiles de consumo individual o familiar y análisis de preferencias, informaciones estadísticas a partir de las informaciones obtenidas gracias a la oferta de servicios[13].

[10] Véase la información publicada en *La Monde,* de 20 de enero de 1996, en primera página.

[11] Observese el significativo titular de *Le Monde.* «Internet contourne la censure du livre du docteur Gubler» 25 de enero de 1996.

[12] Las declaraciones de M. Barbraud, la persona que introdujo el libro en internet a La Monde son paradigmáticas. «A la moindre action de la justice, je bascule mon serveur aux États-Unis, où l'on pourra le consulter au prix de la communication locale», *La Monde,* 25 de enero de 1996.

[13] S. Rodotà, «Tecnologia e Diritti», *Il Mulino,* 1994, pág. 47.

De este modo las tecnologías interactivas crean una nueva «mercancía», y es significativo que cada vez con más frecuencia sean sondeos de opinión y perfiles de consumo los componentes de esa «mercancía».

La dependencia cada vez más estrecha entre la provisión de datos personales y el disfrute de servicios, determinada por la difusión de los medios de comunicación interactivos (televisión por cable, pago por visión, compras a través de Internet) compromete la intimidad y secreto de los datos referentes a la vida privada. Además, el usuario de los servicios informáticos y telemáticos se encuentra en una situación de evidente desigualdad de poder respecto al proveedor de servicios, por lo que no puede hablarse en rigor de un consentimiento libre para las transacciones que se refieren a sus datos personales[14].

Una característica de las redes de telecomunicaciones, y de Internet en particular, es su capacidad de generar una ingente cantidad de datos transaccionales (datos generados a fin de asegurar conexiones correctas). La posibilidad de utilizar las redes de modo interactivo (característica específica de numerosos servicios de Internet) hace aumentar aún más la cantidad de datos transaccionales. Así, al consultar un periódico en línea, el usuario «interactuar» seleccionando las páginas que desea leer, y tal selección crea un «flujo» *(clickstream)* de datos transaccionales. En cambio, los servicios informativos más tradicionales se utilizan de forma mucho más pasiva (la televisión, por ejemplo), limitándose la interactividad al ámbito no automatizado de los kioscos y las bibliotecas.

Por tanto, es posible un conocimiento cada vez más estrecho de sus costumbres, inclinaciones, intereses y gustos. De esto deriva la posibilidad de toda una serie de empleos secundarios de los datos recogidos. Cuanto más sofisticados son los servicios ofrecidos, mayor cuota de información personal deja el individuo en las manos del proveedor del servicio. La riqueza, fiabilidad y tempestividad de los datos recogidos a través de las tecnologías interactivas agravan este problema que se centra en la creación de una nueva mercancía: perfiles individuales y colectivos de usuarios. Cuanto mayor extensión tiene la red de servicios, más crecen las posibilidades de interconexión entre ficheros, o bancos de datos y la diseminación internacional de la información recogida. A dondequiera que se accede en Internet, se deja un rastro digital, de manera que, al ser cada vez mayor el número de actividades de nuestro quehacer cotidiano que se realizan en línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada.

Es posible realizar un seguimiento detallado de las visitas que realiza un usuario sin que éste sea informado de ello mediante el intercambio de los *cookies*. Los *cookies* son pequeños ficheros de datos que se generan a través de las instrucciones que los servidores *web* envían a los programas navegadores, y que se guardan en un directorio específico del ordenador del usuario. Los *cookies* son

[14] *Ibidem*, pág. 54.

algo así como tarjetas de visita de los ordenadores que éstos intercambian entre sí. El concepto y la finalidad del uso de los *cookies* ha cambiado con el tiempo, y ha llegado a ser un poderoso instrumento de obtención de información para el administrador de un servidor y para los departamentos de *marketing* de empresas que hacen publicidad en Internet o simplemente disponen de una página *web*. Los *cookies* pueden contener datos personales o cualquier otro tipo de información relacionada con el interfaz cliente-servidor. Algunos programas navegadores asignan de forma automática el nombre del usuario al fichero que se genera como *cookie*. De esta manera, el nombre del fichero puede estar formado por el nombre del usuario, un símbolo de separación y el nombre del servidor que ha dado instrucciones para generar el archivo *cookie*.

A medida que se desarrollan y popularizan los servicios interactivos, especialmente los que se prestan a través de Internet, crece el problema de la cesión y acumulación de datos personales. Pero los riesgos no provienen sólo de la cada vez mayor cesión de datos personales, sea esta consciente o a través de *cookies*, sino también de la existencia de ciertos programas que hacen búsquedas en Internet con el fin de acumular datos sobre una persona. Un reciente artículo en el *Minneapolis Star Tribune* explicaba como se podía compilar una detallada biografía de una persona elegida al azar utilizando esos programas de ordenador y utilizando la información recogida en los grupos de discusión de la Red en los que participa esa persona. Ese periódico fue capaz de obtener la dirección de la persona, su número de teléfono, lugar de nacimiento, estudios, profesión, lugar de trabajo, su interés en el teatro como aficionado, su tipo favorito de cerveza, sus restaurantes favoritos y lugares de vacaciones y sus puntos de vista sobre varios temas de política de su país. Existen ya algunos sitios de Internet que ofrecen comercialmente este tipo de servicios[15].

Con el fin de hacer frente la creciente amenaza de los servicios interactivos para la vida privada, se han propuesto distintas medidas tanto por parte de las instituciones comunitarias como desde la industria u otras instituciones nacionales.

2.2. Medidas comunitarias para la protección de la vida privada en los servicios interactivos

Las instituciones comunitarias están siendo especialmente activas a la hora de proponer medidas que mejores la tutela de la vida privada en Internet. Las principales medidas adoptadas son de dos tipos: directivas dirigidas a evitar el uso abusivo de los datos, y recomendaciones a usuarios y gobiernos cuyo fin es complementar la acción normativa, dejando en manos de las autoridades nacionales la decisión final sobre estas cuestiones.

[15] Recoge esta información Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales en su Recomendación 3/97 «Anonimato en Internet» de diciembre de 1997», http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp6es.pdf.

Por lo que se refiere a las Directivas podemos mencionar la Directiva 95/46/C.E. relativa a la protección de la personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (D.O.C.E. n.º L 192 de 24 de julio de 1995)[16] y la Directiva 97/66/C.E. del Parlamento y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (D.O.C.E. n.º 24/1, de 30 de enero de 1998)[17].

En estos momentos se está tramitando en el Congreso la adaptación de la L.O.R.T.A.D. a la Directiva 95/46/C.E.[18]. Entre otras modificaciones, deberá limitarse el número de ficheros excluidos de la L.O.R.T.A.D.. Así por ejemplo, los ficheros mantenidos por partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto a los datos relativos a sus asociados, miembros o ex miembros, están excluidos de la aplicación de la L.O.R.T.A.D. (art. 2.2.e de la Ley). Si ya era discutible su exclusión del ámbito de la Ley, la transposición de la Directiva llevará a la obligatoriedad de su inscripción en el Registro de la Agencia de Protección de Datos y su sometimiento al régimen general de la Ley. Además, la Directiva amplia el dato personal susceptible de protección a la imagen y a los sonidos. La utilización de la imagen y del sonido ha experimentado un gran aumento, como en el control de acceso a edificios, la detección de infracciones de tráfico, en los servicios y en el comercio, del que se hace eco la Directiva. Por último, la Directiva establece el denominado derecho de oposición del interesado, que vendrá a sumarse, en el futuro a los ya reconocidos por la L.O.R.T.A.D. (de información, acceso, rectificación, supresión, o el bloqueo de datos). La efectividad de este nuevo derecho exige que se concrete un procedimiento de tutela del mismo.

Un aspecto de la Directiva que está suscitando controversia son las disposiciones relativas a la transferencia de datos personales a terceros países, es decir, países fuera de la Unión europea. La Directiva establece reglas para garantizar que los datos personales sólo van a ser transferidos a terceros países cuando se garantiza una protección similar a la que se garantiza en la Unión Europea, salvo que la transferencia se recoja en una excepción. Si esto no es así, los estados miembros deben informar a la Comisión, que entablará un procedimiento comunitario a permitir que cualquier decisión estatal se extiende al resto de los países la Unión o es revisada.(art. 25 de la Directiva). En espera de la transposición, estos artículo de la Directiva tienen efecto directo, con lo que ello conlleva,

[16] La Directiva puede encontrarse en Internet, http://www2.echo.lu/legal/es/protedat/directiv/directiv.html.

[17] La Directiva puede consultarse en Internet, http://www2.echo.lu/legal/en/dataprot/protection.html.

[18] Sobre las modificaciones que deben ser introducidas en la L.O.R.T.A.D., véase J. J. Martín-Casallo López. «Implicaciones de la Directiva sobre Protección de Datos en la Normativa Española», *Actualidad Informática Aranzadi*, julio 1996, publicado también en *X Años de Encuentros sobre Informática y Derecho (1996-1997)*, Aranzadi, 1997, pág. 75.

desde el 24 de octubre de 1998. Debido a las enormes implicaciones que estas normas tienen para las empresas, el art. 26 permite a las compañías establecer ellas mismas mecanismos que garanticen que el flujo de datos respeta los principios de la Directiva. La importancia de estas limitaciones al flujo de datos aumenta si se tiene en cuenta que la Directiva se aplica también a los flujos de datos en Internet. Las soluciones técnicas, como los mecanismos que informan a los consumidores y obtienen su consentimiento para el procesamiento de datos, serán especialmente útiles para evitar la prohibición de exportación de datos[19]. Estas disposiciones han comenzado por causar malestar entre las compañías norteamericanas que operan en Europa, ya que el 23 de noviembre la Comisión europea anunció que la propuesta del Ministerio de comercio norteamericano no era suficiente para garantizar el no abuso de los datos. La propuesta norteamericana consistía en la autorregulación voluntaria por las empresas. Las compañías y el gobierno norteamericano perciben la regulación comunitaria como un intento de exportar la regulación europea de la vida privada a otros países, ya que si éstos quieren operar con normalidad en Europa, deberán tarde o temprano ajustar sus legislaciones a los requisitos de la Directiva. En este sentido, el gobierno australiano ha declarado que está considerando la adopción de una legislación en la materia para cumplir con los requisitos que exige la Directiva. El gobierno de Estados Unidos entiende también que este la regulación de la Directiva es una barrera comercial, al estar en juego billones de dólares. Finalmente existe la amenaza latente de que el gobierno norteamericano denuncie esta regulación ante los órganos de composición de diferencias del G.A.T.T., o que aplique sanciones selectivas a las empresas europeas que operan en Estados unidos en lo que empieza a conocerse como «La guerra de los datos»[20].

Otra importante Directiva es la 97/66/C.E. del Parlamento y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (D.O.C.E. núm. 24/1, de 30 de enero de 1998). Esta acción de la Comunidad pretende dar un primer paso armonizador frente a las necesidades específicas en materia de protección de datos personales e intimidad que generan los nuevos servicios interactivos que se prestan a través de la Red Digital de Servicios integrados y los teléfonos móviles. Como se ha dicho, los riesgos más importantes que presentan los servicios interactivos tienen que ver con el almacenamiento y el tratamiento informático de datos relativos a abonados y usuarios. La Directiva contiene disposiciones que conciernen varios temas: seguridad de la información transmitida a través de las redes públicas de comunicación; confidencialidad de las comunicaciones; limitaciones a la capacidad de proceso de datos sobre el tráfico y los recibos por los proveedores de los servicios; opciones del usuario sobre la identificación de la línea llamante y la línea conectada; protección de los consumi-

[19] Véase el documento informativo de la Comisión Europea «Data Protection: Background Information», http://europa.eu.int/comm/dg15/en/media/dataprot/info.htm.

[20] Véase http://www.inforsecuritymag.com/feb99/datawars.htm.

dores frente a llamadas automáticas o llamadas no solicitadas; y derecho de los abonados de no aparecer en listados públicos.

La Directiva establece que los proveedores de servicios deben tomar las medidas adecuadas para salvaguardar la seguridad de los servicios e informar a los abonados al servicio de todo riesgo concreto de violación de la seguridad de la red. En el caso concreto de violación de la seguridad de la red, el proveedor de un servicio de telecomunicaciones deberá informar a los abonados sobre ese riesgo.

Por lo que se refiere a la confidencialidad de las comunicaciones, se establece que los Estados miembros destinatarios de la Directiva, deberán garantizar la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicación. En particular, deberán prohibir la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, salvo que estén autorizadas legalmente.

Los datos de tráfico relacionados con los usuarios y abonados para establecer comunicaciones y almacenados por el proveedor de la red deberán destruirse o hacerse anónimos al acabar la comunicación. Además, el tratamiento de los datos de tráfico y facturación deberá limitarse a las personas que actúen bajo las órdenes del proveedor de la red, que se ocupe de la gestión de la facturación o tráfico, solicitudes de información de los clientes, detección de fraudes y promoción comercial de los propios servicios del proveedor.

Por lo que se refiere a las opciones del usuario sobre la identificación de la línea llamante y la línea conectada, la Directiva contiene varias disposiciones regulan la posibilidad de suprimir la identificación de la línea llamada y de la línea conectada, tanto para el emisor como para el receptor de la llamada. En el caso de llamadas maliciosas y molestas, la propuesta de Directiva establece que por un periodo de tiempo limitado, los datos que incluyan la identificación del abonado que origina la llamada sean almacenados y puestos a disposición de acuerdo con el Derecho nacional.

En cuanto a los sistemas de llamada automática, con fines de venta directa, se establece que sólo se podrán autorizar respecto de aquellos abonados que hayan dado su consentimiento previo. Además, los Estados tomarán las medidas adecuadas para garantizar gratuitamente que no se permitan las llamadas no solicitadas con fines de venta directa por otros medios, sin el consentimiento de los abonados.

La Directiva contiene también disposiciones que se refieren a las guías o listados públicos de usuarios. Los datos personales recogidos en las guías impresas o electrónicas accesibles al público, o que puedan obtenerse a través de servicios de información se limitarán a lo estrictamente necesario para identificar al abonado. Además, el abonado tendrá derecho de forma gratuita, a que se le excluya de la guía impresa o electrónica a petición propia, a indicar que sus

datos personales no se utilicen para fines de venta directa, a que se omita parcialmente su dirección y a que no exista referencia que revele su sexo.

En cuanto a las recomendaciones de la Comisión o de otras instituciones comunitarias podemos mencionar las recomendaciones del Grupo de Trabajo sobre protección de los individuos respecto al procesamiento de datos personales. Este Grupo de Trabajo ha hecho públicas algunas recomendaciones sobre transferencia de datos a terceros países e intimidad e Internet. Es particularmente interesante la Recomendación 3/97 sobre el anonimato en Internet[21]. la recomendación percibe el anonimato en Internet como una eficaz protección de la vida privada en Internet. La acumulación de datos personales sólo supone un riesgo para la vida privada cuando se identifica a la persona a la que se refieren los datos. La máxima que debe valer para Internet es que si el usuario puede mantener el anonimato fuera de línea, deberá ofrecérsele la misma posibilidad en línea, tal y como se afirma en la «Declaración Ministerial de Bonn»[22]. En concreto la Recomendación estudia los distintos mecanismos que favorecen el anonimato tanto en el uso del correo electrónico como en grupos de discusión, salas de charla, al navegar por Internet y en la adquisición de bienes y servicios a través de Internet.

2.3. Propuestas de otras instituciones.

A parte de esta regulación que proviene del derecho comunitario, puede destacarse la iniciativa de la Asociación Española de Comercio Electrónico, para la creación del Código Ético de protección de Datos Personales en Internet[23], que ha recibido el respaldo y la aprobación de la Agencia de Protección de datos. Al Código pueden adherirse todas las empresas que lo deseen, que de este modo están vinculadas por él. Como contrapartida, las empresas pueden utilizar el sello de garantía de protección de datos. El Código establece la obligación de todas aquellas empresas que capten datos personales de informar el uso que hacen de esos datos. Antes de cualquier transferencia de datos deberán advertir a los dueños de esos datos para darles la oportunidad de prohibir la cesión. Uno de los principios del Código ético es permitir las mayores facilidades para negarse a la recogida o cesión de datos. También se establecen medidas específicas para garantizar que la publicidad sólo se va a enviar a clientes que no hayan manifestado su oposición. Las ofertas en línea deben identificarse claramente como tales, revelando asimismo la identidad del anunciante. Donde sea posible, los consumidores deberán disponer de la opción a negarse a través del correo electrónico. El Código incluye también disposiciones sobre la captación de datos de menores. El control del cumplimiento de las normas del código ético se enco-

[21] En Internet: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp6es.pdf.

[22] Declaración Ministerial de la Conferencia Ministerial sobre Redes mundiales de información, celebrada en Bonn los días 6 a 8 de julio de 1997.

[23] http://www.aece.org/corporativo/codigoetico.doc

mienda al Comité de protección de datos de la A.E.C.E., creado por el propio Código.

La Agencia de Protección de Datos publica periódicamente recomendaciones y consejos para preservar la intimidad frente a la acumulación de datos personales. Un ejemplo de ello es la «Recomendación a Usuarios de Internet»[24], en los que la Agencia hace unas recomendaciones generales muy útiles.

3. La encriptación

El problema de la seguridad en las transmisión de información concierne numerosos servicios de pago, como la televisión. El uso de codificadores comenzó a principios de los años 80 para evitar la recepción indiscriminada de imágenes. La codificación de la información consiste en un mecanismo que altera la imagen y el sonido antes de la transmisión para que un receptor normal no pueda reconstruir el programa original. Para reconstruir la imagen, el usuario necesita un descodificador especial. La codificación de señales de televisión comenzó en el sector de la televisión por cable y su uso se ha incrementado enormemente con la transmisión de televisión vía satélite. Actualmente se trata de un mercado en plena expansión debido a los nuevos servicios de radiodifusión que permite la digitalización, como el pago por consumo o por visión *(pay per view)*, y el vídeo casi bajo demanda *(video nearly on demand)*. Aun así, existe una creciente preocupación a nivel europeo por la creación de una industria paralela especializada en aparatos piratas de descodificación. Según cálculos de la Comisión europea, entre un 5% y un 20% de los descodificadores no están autorizados[25].

Por otro lado, aun existiendo importantes leyes que protegen la confidencialidad de las comunicaciones, los medios de comunicación son cada vez más vulnerables. La red telefónica se ha convertido en un sistema de comunicación en el que es prácticamente imposible garantizar la absoluta confidencialidad de las llamadas. Las escuchas telefónicas son fáciles de realizar. En especial, el creciente uso de la telefonía móvil e inalámbrica, que utiliza el espectro radioeléctrico hace particularmente vulnerables a las intercepciones estas comunicaciones.

Numerosos datos sensibles como los números de tarjetas de crédito son transmitidos continuamente a través de canales inseguros como los teléfonos móviles o Internet. El problema es aún más grave para las empresas. Durante los años 70, los ejecutivos de I.B.M. realizaron miles de llamadas telefónicas a través de la red privada de la compañía y esas llamadas eran sistemáticamente interceptadas por los servicios de inteligencia de la Unión Soviética. Las redes informáti-

[24] Una versión reducida se encuentra en http://www.ag-protecciondatos.es/recomen.html.

[25] Comisión Europea, Legal Protection for Encrypted Services in the Internal Market. Consultations on the Need for Community Action. 6.3.96. Véase también el Dictamen del Comité Económico y Social sobre el Libro Verde de la Comisión, D.O.C.E. serie C 30, de 30 de enero de 1997, pág. 10.

cas son especialmente vulnerables a la intercepción. Recientemente se ha descubierto que algunos empleados de *British Airways* han accedido continuamente a los registros de pasajeros de la compañía *Virgin Atlantic.* A partir de esa información, *British Airways* ha llevado a cabo intentos sistemáticos para convencer a los pasajeros de esa compañía para cambiar a *British Airways*[26].

Debido a esta situación, los usuarios de redes de telecomunicaciones especialmente empresas que desean proteger secretos comerciales y de información interna, han ido exigiendo mayor protección de las comunicaciones. Una respuesta a la creciente demanda de seguridad en las comunicaciones es la encriptación[27]. La encriptación es el arte de crear y usar métodos para disfrazar mensajes usando códigos, algoritmos y otros métodos de tal modo que sólo las personas que conocen esos códigos pueden acceder a la información.

La encriptación ha sido usada desde hace tiempo en aplicaciones militares para garantizar la transmisión de información sensible a través de canales inseguros. La moderna encriptación usa algoritmos, que tan sólo pueden ser leídos y descifrados por aquellos a los que va dirigido. Un algoritmo es una función matemática usada para codificar y descodificar un mensaje. Cada algoritmo poseen una clave que sólo es conocida por los interesados. Actualmente, la encriptación es usada por los particulares, que pueden de este modo proteger sus comunicaciones, sobre todo su correo electrónico. La encriptación puede ser aplicada a cualquier tipo de comunicación digital: teléfonos, faxes, comunicaciones por satélite. Aparte del creciente uso de la encriptación por los particulares, ésta cumple un papel fundamental en numerosas aplicaciones comerciales. Las principales aplicaciones comerciales son las siguientes[28]: descodificadores de televisión por satélite, cajeros automáticos, transferencia electrónica de dinero, la red SWIFT, la telefonía GSM y las tarjetas telefónicas, llaves de cierre remoto en coches, etcétera.

Los principales aspectos que garantiza la encriptación son la confidencialidad, la integridad y la autenticidad de la información. El servicio que se asocia más frecuentemente con la encriptación es la transformación de la información de manera que resulta ininteligible para todo aquel que no sea el destinatario de la misma. La encriptación otorga una total seguridad a estas transacciones. No sólo evita que los mensajes, de cualquier tipo que sean, puedan ser conocidos por personas ajenas a la comunicación, sino que otorgan una fiabilidad absoluta sobre la veracidad de esos datos.

---

[26] Estos dos ejemplos aparecen citados en el trabajo «Codes, Keys and Conflicts: Issues in U.S. Cryptopolicy» http://info.acm.org/reports/acm_crypto_study.html, capítulo primero.

[27] Sobre este tema hay un número creciente de artículos, sobre todo en Internet. M. Frommkin. «The Methaphore is the Key: Criptography, the Clipper Chip, and the Constitution», http://www-swiss.ai.mit.edu/6095/articles/froomkin-metaphore/text.html.

[28] J. Dávila, J. L. Morant y J. Sancho. «Control Gubernamental en la Protección de Datos: Proyecto Clipper», *X Años de Encuentros sobre Informática y Derecho. 1996-1997,* Aranzadi, 1997, pág. 42.

Por lo que se refiere a la integridad de la información transmitida, se trata de un servicio garantizado por la encriptación, que permite al usuario detectar si la información ha sido alterada durante su transmisión o almacenaje. Relacionada íntimamente con la integridad, se halla la garantía de la autenticidad de la información. La autenticidad permite identificar al emisario de la información. La autenticación pasa frecuentemente a través de la asociación de una clave de encriptación con un usuario, lo que a veces se conoce como firma digital. Actualmente existe una propuesta de Directiva comunitaria sobre firma digital que se estima es imprescindible para permitir el comercio electrónico en Internet[29] Integridad y autenticación se asocian frecuentemente. Sin embargo una información de la que se garantiza su autenticidad y su integridad puede no ser confidencial. Mientras que los servicios de autenticación e integridad no plantean problemas importantes, el servicio de confidencialidad garantizado por la encriptación puede resultar conflictivo.

Los programas de encriptación son productos comercializados por empresas especializadas aunque algunos de ellos se distribuyen libremente en Internet por ser *freeware.* Este es el caso de P.G.P. P.G.P. son las siglas *de Pretty Good Privacy*, un programa de encriptación de mensajes de correo electrónico. Debido a la inseguridad que supone el envío de mensajes a través de Internet, ya que pueden ser interceptados y leídos por cualquiera en cualquier servidor por los que pasen, P.G.P. permite codificarlos con una potente clave. P.G.P. emplea un sistema de clave pública, lo que hace posible combinar la potencia de la encriptación convencional con su fácil uso a través de Internet. El usuario dispone de dos claves: una clave secreta y una clave pública para que puedan enviarle mensajes. El emisor codificará su mensaje con la clave pública del destinatario. Para descodificar el mensaje, el destinatario deberá emplear su clave secreta, de la que sólo él tiene copia.

Una vez más hay que tener en cuenta que Internet es una red que no conoce fronteras de ningún tipo y que con la misma facilidad se accede en unos segundos tanto a una página *web* en España como a una en Australia, aunque las dos acciones puedan tener consecuencias jurídicas muy distintas. El uso de P.G.P. está prohibido en varios países, por lo que enviar un mensaje codificado con P.G.P. a un usuario de China, o incluso de Francia, puede causar graves problemas legales a su destinatario. Además, el Gobierno de Estados Unidos impone límites de exportación a la tecnología del encriptado, como ha sido apuntado, equiparándola a armamento. Por ello, la obtención de una copia de P.G.P. de una página *web* de Estados Unidos puede también dar lugar a complicaciones legales.

P.G.P. es fácil de manejar y emplea un algoritmo de encriptación muy difícil de romper actualmente. Al crecer el lado comercial de Internet, y al tener lugar

[29] Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica, de 5 de mayo de 1998.
http://www.europa.eu.int/comm/dg15/en/media/infso/com297en.pdf

en él un número creciente de transacciones comerciales, la seguridad de éstas se convierte en un tema esencial de la Red. La encriptación es el instrumento más eficaz que los usuarios pueden emplear para garantizar la seguridad en las transacciones, no sólo en Internet, sino en todo tipo de comunicaciones electrónicas. El recurso más importante para garantizar la seguridad en Internet consiste en codificar los mensajes de tal forma que únicamente quien los envía, y quien debe recibirlos puedan entenderlos. Como hemos visto, se ha desarrollado una industria paralela a la de los programas habituales para poner en clave la información cibernética. La existencia de esta tecnología es un factor clave para el crecimiento futuro de Internet como motor del comercio y la comunicación internacionales.

3.1. Dos intereses en conflicto debido a la encriptación: el derecho a la inviolabilidad de las comunicaciones y el interés del Estado en la aplicación de la Ley

La encriptación es una ciencia en constante evolución[30]. Esta evolución consiste en el uso de algoritmos cada vez más complejos que permiten aumentar continuamente su seguridad frente a posibles quebrantamientos. Los particulares, y especialmente las empresas, exigen una encriptación cada vez más potente. Las técnicas de encriptación más recientes ofrecen un grado tan alto de seguridad en la comunicación que han despertado el recelo de los gobiernos sobre su uso para comunicaciones ilícitas. La perspectiva de la toma de un edificio por unos terroristas que usen programas de cifrado potente en sus comunicaciones telefónicas ha hecho reaccionar a varios gobiernos, que tratan de buscar soluciones para evitar usos ilegítimos de las técnicas de encriptación. En especial, el gobierno Estados Unidos, en donde se halla el mayor número de usuarios de encriptación y de empresas especializadas en estos servicios, baraja distintas posibilidades para controlar su uso por los particulares. El problema fundamental que plantea la encriptación es, paradójicamente, el de su fiabilidad.

El debate generado por la encriptación se centra en el conflicto entre la creciente demanda de garantía de la seguridad de las comunicaciones y la necesidad de garantizar que esas técnicas no supongan un obstáculo insalvable para la aplicación de la Ley, y en definitiva proteger la seguridad nacional.

El temor que genera la encriptación es real, hasta el punto de que hay países que han prohibido su uso. No obstante, cualquier intento de restringir el uso civil de la encriptación se enfrenta a intereses comerciales muy fuertes por parte de bancos, sector servicios, emisoras de televisión, grandes compañías, etc. En aquellos casos en los que los gobiernos han tratado de prohibir la encriptación civil, han tenido que retirar sus propuestas, como es el caso de Holanda en 1994. La prohibición del uso de la encriptación civil es común en países en los que

[30] Un análisis detallado de la historia de la encriptación y de los problemas que genera, puede encontrarse en «Codes, Keys and Conflicts: Issues in U.S. Cryptopolicy» http://info.acm.org/reports/acm_crypto_study.html.

el Estado ejerce un fuerte control sobre sus ciudadanos como China, Corea del Sur y Taiwan.

En la Unión Europea la encriptación recibe un distinto tratamiento en cada uno de los niveles de creación de normas, y dependiendo también de si se trata o no de encriptación fuerte. La encriptación fuerte está regulada en un cuerpo normativo encabezado por el «Arreglo de Wassenar»[31], de 1995 que la define como una mercancía de «doble uso». Se trata de un convenio internacional multilateral que regula la comercialización, importación y exportación de productos bélicos y tecnología asimilada que es la tecnología de doble uso. A través del «Acuerdo de Wassenar» se imponen restricciones a la exportación de las mercancías de doble uso.

Aparte de estas disposiciones sobre encriptación fuerte, la Comisión europea está impulsando varios proyectos que propiciarán la creación de un sistema de licencias de empresas que proporcionen encriptación en Europa, que se conoce como *T.T.P. (Trusted Third Parties)*, y que es analizada más adelante. Esta propuesta, que se discute en estos momentos en varios países europeos, se basa en la concesión de permisos a las compañías que ofrecen sus servicios de encriptación. De este modo, el control del Estado garantizaría la necesaria confianza de los usuarios en estas empresas, a la vez que permitiría que la interceptación legal de la comunicación.

El segundo foro europeo para la discusión de los temas relacionados con la encriptación es la O.C.D.E., Organización para la Cooperación y el Desarrollo en Europa. La O.C.D.E. ha establecido un Grupo de Expertos para estudiar las implicaciones de la encriptación. El Grupo de expertos elaboró un documento con unas directrices para los Estados. El documento del Grupo de Expertos establece ocho aspectos clave que conciernen la encriptación: la confianza en los métodos de encriptación, la elección entre distintos métodos a disposición del usuario, las tendencias del mercado en el desarrollo de sistemas de encriptación (que deben primar frente a las proposiciones de los gobiernos), los estándares de encriptación que deben permitirse, la responsabilidad que debe recaer sobre las empresas de encriptación, la protección de la vida privada y de los datos personales, la interceptación lícita de la comunicación y la necesidad de cooperación a nivel internacional.

Francia tiene una de las legislaciones más restrictivas de Europa, al equiparar la encriptación a material bélico, y, por tanto, al requerir autorización expre-

[31] Puede encontrarse en Internet en htto://www.onnet.es/03005007.htm. El Acuerdo ha sido completado y desarrollado por el Real Decreto 491/1998 sobre Comercio Exterior en material de Defensa y Doble Uso, de 27 de marzo (B.O.E. 8-4-1998). Aparte de este «Arreglo», existe una Decisión adoptadas en el ámbito de Cooperación de Política Exterior y de Seguridad Común de la Unión Europea (P.E.S.C.), que limita la exportación de las mercancías de doble uso fuera del espacio de la Unión Europea. Se trata de la Decisión 94/942/P.E.S.C. Además, existe un Reglamento comunitario por el que se restablece el régimen comunitario de control de las exportaciones de productos de doble uso Reglamento C.E./3381/94.

sa del Primer Ministro para su exportación, salvo que se trate de encriptación que garantice sólo la autenticación. También, Francia prohibe el uso de material de cifrado si no se ha registrado el algoritmo. Rusia considera ilegal el uso de encriptación si no se ha obtenido una licencia para su uso. El Reino Unido está actualmente preparando una legislación específica[32], que prohibirá el uso comercial de encriptación si no se ha obtenido la correspondiente autorización (sistema T.T.P.). También se prohibirá la comercialización de encriptación que se ofrece a usuarios en el Reino Unido a través de Internet. Otros países como Alemania o los países nórdicos no tienen restricciones para el uso de la encriptación, aunque en Alemania, una reciente ley fuerza a todas las compañías de telecomunicaciones a establecer mecanismos que garanticen la interceptación legal de las comunicaciones[33].

En España la normativa que regula la encriptación se basa en el art. 52 de la ley General de Telecomunicaciones, de 1998 que consagra, en principio, la libertad de encriptación para todo tipo de mensajes. No obstante, en el párrafo segundo el art. 52 establece que se podrá imponer la obligación de notificar, bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos a efectos de su control de acuerdo con la normativa vigente. la referencia de este segundo párrafo se refiere al previsto en el Reglamento de Comercio Exterior de material de Defensa y de Doble Uso establecido por Real Decreto 491/1998, pero abre una posibilidad de otras medidas de limitación como la *key scrow,* que es analizada posteriormente.

En Estados Unidos se halla el mayor número de usuarios de encriptación, aunque su uso se ha extendido rápidamente entre los usuarios de Internet de todo el mundo. Un primer aspecto llamativo de la regulación norteamericana de la encriptación es la prohibición casi total de exportación del material de cifrado fuerte. En julio de 1998 un juez norteamericano prohibió a un profesor de universidad publicar *software* cifrado en su página *web,* cuyo fin era enseñar a sus estudiantes estadounidenses y extranjeros tecnología de seguridad. El profesor apelaba a que estos programas debían estar protegidos por la libertad de expresión. la decisión judicial, sin embargo, considera que estos programas no están amparados por la Primera Enmienda a la Constitución Americana, que recoge la libertad de expresión, ya que no son comprensibles para la mayoría de las personas. El profesor pretendía desafiar las restricciones sobre este tipo de tecnología, la cual requiere una licencia de exportación al ser equiparada a la tecnología militar[34]. La encriptación fuerte se asimila para su exportación al

[32] Véase el informe preparado por el Gobierno del Reino Unido, «Licensing of Trusted Third Parties for the Provision of Encryption Services», http://www.dti.gov.uk/pubs

[33] J. Dávila, J. L. Morant y J. Sancho. «Control Gubernamental en la Protección de Datos: Proyecto Clipper», *X Años de Encuentros sobre Informática y Derecho. 1996-1997,* Aranzadi, 1997, pág. 44

[34] Más información sobre este caso en http://www2.echo.lu/legal/en/news/9808/chapter11.html#2. La sentencia puede consultarse en http://jya.com/pdj11.htm. Actualmente existe un proyecto de ley de 12 de mayo de 1998 en el Senado norteamericano conocido como E-PRIVACY Act

comercio de armas en Estados Unidos, lo que está provocando que otros países con una legislación más favorable a la exportación de este tipo de productos como Alemania, Suiza o Bélgica obtengan pingües beneficios en el creciente mercado de la encriptación.

3.2. Algunas propuestas para resolver el conflicto: El *Key Scrow System* de Estados Unidos

En Estados Unidos surgió la iniciativa de encriptación llamada *Clipper* o *Key Escrowed System* (Sistema de Claves Depositadas)[35], destinada a proporcionar a los usuarios civiles de la encriptación un alto nivel de seguridad en las comunicaciones, haciendo especial hincapié en la confidencialidad de las mismas, sin que ello supusiera frustrar la legítima acción del Estado cuando la interceptación de la comunicación fuese preceptiva. Esta iniciativa se basa en dos elementos: un chip cifrador a prueba de análisis o manipulación y un sistema de depósito de las claves secretas, que, en determinadas circunstancias, otorgaría al Gobierno el acceso a la clave maestra de cada chip, permitiendo descifrar la comunicación.

Cada clave secreta se divide en dos componentes que se entregan a dos agencias estatales depositarias independientes para su custodia. Sólo en el caso de que sea necesaria la interceptación de la comunicación y tras obtener la preceptiva autorización judicial, la policía puede conseguir de las dos agencias los dos componentes cifrados de la clave que permite descifrar la comunicación. En el momento de interceptar una comunicación, se siguen un protocolo en tres fases[36]:

1. Si durante una escucha legal se detectan comunicaciones cifradas mediante el sistema *Clipper*, se solicita a las dos Agencias Depositarias que proporcionen a los agentes las dos partes de la clave. Para ello es necesario que junto a la preceptiva autorización judicial, se aporte cierta información sobre los chips.
2. Las dos Agencias Depositarias extraen los componentes cifrados de la clave y los entregan a los agentes. Las dos partes de la clave se introducen en un procesador de descifrado para que se la clave pueda ser reconstruida. Obtenida la clave, nada impide ya descifrar las comunicaciones.
3. Al terminar la escucha, los agentes ordenan al procesador que borre la clave del procesador de descifrado. Sería ilegal que la clave descifrada permaneciera en el procesador de descifrado más allá del tiempo permitido para la escucha en la autorización judicial. En el momento en que el procesador

(que es el acrónimo de: *Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace*). Si este proyecto de ly es aprobado se relajarían las restricciones a la exportación de criptografía para uso civil. Más información sobre este proyecto de ley, http://www2.echo.lu/legal/en/news/9806/chapter11.html#3. Was introduced in the U.S. Senate on 12 may 1999

[35] *Ibidem*, 25.

[36] *Ibidem*, pág. 36.

de descifrado ha borrado esa información, éste genera y envía de modo autónomo un certificado de la destrucción de la clave a las Agencias Depositarias.

El *Clipper* es, hasta el momento, un estándar de cifrado voluntario en Estados Unidos para las comunicaciones telefónicas, incluyendo voz, fax y datos. Se pretende que, a pesar de su carácter voluntario, se extienda hasta convertirse en el estándar de cifrado por excelencia, capaz de conjugar los intereses de los particulares de confidencialidad y los intereses del Estado en garantizar la aplicación de la ley.

A pesar de los intentos por parte del Gobierno norteamericano para que la propuesta *Clipper* fuese aceptada, han surgido numerosas críticas. La primera objeción que se ha hecho a *Clipper* es la relativa a cual sea la verdadera intención de una implantación masiva de un sistema de claves depositadas, ya algunos no consideran probada que la intención sea la defendida públicamente de proteger el secreto de las comunicaciones al mismo tiempo que las intervenciones judiciales. Aquellos contrarios al proyecto *Clipper* ven en él una potencial amenaza contra la libertad individual por parte del Estado. En especial, los grupos de defensa de los derechos civiles en Estados Unidos, incluida *la American Civil Liberties Union* (A.C.L.U.) consideran que el *Clipper* constituye una intromisión intolerable en el derecho a la vida privada de los ciudadanos y que se trata de un paso más del Estado para controlar la vida de los ciudadanos[37].

En segundo lugar, se argumenta que las Agencias Depositarias están expuestas a ataques al concentrar en ellas información de alto interés. Es decir, no se garantiza la invulnerabilidad de las Agencias Depositarias, por lo que el *Clipper* pierde fiabilidad. La propuesta *Clipper* es muy criticada al hacer vulnerable, y por tanto, hacer perder valor, a la encriptación.

3.3. El sistema T.T.P. (*Trusted Third Parties*)

El sistema T.T.P.[38] se basa en la existencia de una empresa autorizada por el Estado, a las que se encomienda la seguridad y condifencialidad de las telecomunicaciones. En realidad se trata de una empresa que ofrece un servicio de valor añadido a aquellos usuarios que desean aumentar la fiabilidad de los servicios que reciben. La diferencia con el proyecto *Clipper* es patente, desde el momento en que ya no se trata del depósito de las claves de la comunicación en un organismo público, sino que se encomienda a empresas que ofrecen este servicio de valor añadido. Actualmente, países como Francia, Reino Unido o Alemania tienen una legislación de tipo T.T.P., o bien están considerando su adop-

[37] «Codes, Keys and Conflicts: Issues in U.S. Cryptopolicy» http://info.acm.org/reports/acm_crypto_study.html. capítulo 8.

[38] Más información sobre T.T.P. en el informe preparado por el Gobierno del Reino Unido, «Licensing of Trusted Third Parties for the Provision of Encryption Services», http: //www.dti.gov.uk/pubs.

ción. A su vez, la Comisión europea ha puesto en marcha varios proyectos piloto con el fin de implantar en el futuro u sistema T.T.P. a nivel europeo.

Las ventajas del sistema T.T.P. son las varias: las empresas que ofrecen este servicio de valor añadido deben contar con un título (licencia, autorización, concesión) que les permita ofrecer sus servicios. De este modo existe un control por parte del Estado sobre estas empresas. Además, esta iniciativa puede resolver el problema de confiar las claves a una agencia estatal, al tratarse de empresas privadas, aunque en el caso de que sea precisa la interceptación de la comunicación, la autorización judicial obligaría a la empresa a entregar las claves. En este sentido, el Reino Unido está estudiando, como uno de los requisitos para obtener el título, el que la empresa pueda entregar las claves en un tiempo inferior a una hora, desde que se le entrega la autorización judicial.

El sistema T.T.P. puede adoptarse, prohibiendo la comercialización de cualquier producto de cifrado que no conste con el preceptivo permiso, es decir, excluyendo el uso de encriptación que no conste con autorización del Estado, como es el caso de Francia, o puede implantarse permitiendo que conviva con otros tipos de encriptación que no se comercialicen, y que aspire a sustituir a éstos, como es la intención del Reino Unido. Esta última posición permite el uso de sistemas que actualmente pueden obtenerse gratuitamente en Internet y que son ampliamente usados en todo el mundo, como es el caso de P.G.P. *(Pretty Good Privacy)*.

4. CONCLUSIONES

Las nuevas tecnologías e Internet permiten nuevas posibilidades de comunicación que antes sólo podían ser soñadas. No obstante, las nuevas tecnologías e Internet presentan también nuevos riesgos que consisten en una mayor capacidad de control sobre los individuos. A veces la impresión que ofrecen las nuevas posibilidades de acumulación de datos y de elaboración de perfiles es la de «desnudez de la vida privada». Pero si el objeto de las pesadillas orwellianas era el estado controlador, los sujetos frente a los que hay que proteger al individuo en la sociedad de la información son, más bien, las grandes compañías y corporaciones que acumulan y trafican con los datos de millones de personas. La información sobre los individuos, su salud, inclinaciones políticas y sobre todo pautas de consumo, se han convertido en una mercancía muy valiosa. la tarea del legislador consiste en obtener un adecuado equilibrio entre el interés creciente que tiene la sociedad en la circulación de la información sobre los individuos y la protección de la vida privada, que se tutela en nuestro ordenamiento a través de varios derechos fundamentales recogidos en el art. 18 de la Constitución. Como establece la Constitución en su art. 10 la dignidad de la persona y el respeto a de los derechos inviolables que le son inherentes constituye el fundamento del orden político y la paz social.