

# Protección de la intimidad en Internet

CINTA CASTILLO JIMÉNEZ

*Profesora de Derecho Informático de la Universidad de Sevilla*

Factores como la velocidad, la potencia y la capacidad de almacenamiento de los ordenadores, son hoy en día una seria amenaza a la intimidad o privacidad de las personas, riesgo que se ve aumentado cuando se facilita la comunicación entre terminales separados por miles de kilómetros, no existiendo ningún impedimento técnico para el tratamiento de datos personales.

Las legislaciones y la jurisprudencia de los Tribunales de los países de la Unión Europea y de E.E.U.U., han primado el reconocimiento del Derecho a la intimidad como valor esencial, que debe protegerse ahora de manera especial por el continuo avance tecnológico y sus repercusiones.

Los principios básicos de la protección son de naturaleza general y se aplican a todas las tecnologías de la información, por tanto a todos los tipos de redes, abiertas o cerradas, incluyendo Internet y sus integrantes; proveedores de acceso, proveedores de servicios y usuarios.

Las Leyes de protección de datos personales informatizados, que nacen para proteger al titular de la información en lo que se refiere a su intimidad personal, restringen la circulación no autorizada de datos que puedan representar una invasión de la esfera privada. En lo que se refiere a Internet, se recomienda ampliamente a los usuarios, negociantes u operadores tomar todas las medidas

necesarias antes de divulgar un texto o imagen que pueda suponer una violación del derecho a la intimidad. En este sentido, se hizo patente la amenaza al derecho a la intimidad, cuando se publicó en el Web de Internet, el libro del Dr. C. Gubler y Mr. Gonod sobre la historia médica y política del que fue presidente de la república francesa, François Mitterand. El libro titulado *Le grand secret*, estuvo disponible en Internet sólo unos días, después de que se prohibiera su venta en las librerías, y violando los derechos de autor reconocidos en las Leyes de propiedad intelectual.

Con este suceso, una vez más, se abre el eterno debate en el que se discute sí el derecho a la intimidad limita la libertad de expresión del autor que, respecto a asuntos que puedan considerarse de interés público, puede reforzarse con el argumento del derecho del público, de los ciudadanos a la información. Todo ello, teniendo en cuenta el respeto de la intimidad de un Jefe de Estado y de su familia. Entre estos dos derechos existe un delicado equilibrio, que debe ser valorado por los jueces caso por caso para decidir en cada momento cual de estas libertades y valores prevalece.

Internet no ha aportado nada nuevo al conflicto de intereses que acabamos de esbozar, eso sí, ha hecho posible la difusión sin fronteras temporales ni espaciales de informaciones con las cuales se está dejando sin contenido la protección y garantía de derechos fundamentales, reconocidos por todas las legislaciones.

Los usuarios de la red de redes, hacen circular archivos, expedientes o correo electrónico que contiene información personal susceptible de protección, ya sea referente a autoridades públicas o bien, entre usuarios particulares.

La legislación europea y americana hacen distinción según se trate de uno u otro grupo. En la legislación de EEUU y Canadá la protección de la intimidad en la esfera pública está garantizada como un derecho constitucional de aplicación a las comunicaciones electrónicas y por tanto, a Internet. Esta protección constitucional se aplica a los órganos gubernamentales.

Las leyes que protegen el derecho a la intimidad en este ámbito en EEUU, (Electronic Communications Privacy Act) y en Canadá (el Criminal Code), requieren autorizaciones para las comunicaciones electrónicas, de forma que la policía no puede interceptar el contenido del correo electrónico ni hacer transferencias a través de FTP o Telnet sin una orden.

La ECPA, prohíbe el acceso, sin orden de búsqueda a la información almacenada en un ordenador, sin embargo faculta a las autoridades relacionadas con el Ministerio de Justicia a emplear dispositivos técnicos que graban los números marcados desde un teléfono, o bien, los números telefónicos de todas las personas que marquen un teléfono dado. Con la aplicación de estas medidas en Internet las autoridades no necesitarían una orden de búsqueda para la identificación de ordenadores que establecen conexión con otros que están bajo vigilancia.

La legislación europea contempla en los ordenamientos de cada uno de los países la protección que dan las distintas Constituciones y el resto de las normas dedicadas a la protección de la intimidad, así como el Convenio europeo de derechos humanos, éste limita las medidas adoptadas por las leyes nacionales de los Estados firmantes para permitir el acceso a las comunicaciones en general, y las comunicaciones en Internet en particular, por parte de las autoridades gubernamentales. En la sección octava de este Convenio se garantiza el derecho a la intimidad y confidencialidad de la correspondencia, esto supone por un lado, que las autoridades públicas deben garantizar el respeto a la intimidad entre los ciudadanos, y por otro, que deben abstenerse por sí mismas de toda interferencia, a menos que se den las circunstancias excepcionales que deben estar prescritas por la Ley. Esta interferencia a la que nos referimos debe ser necesaria y proporcionada por las normas de una sociedad democrática, y tener como objetivo la seguridad nacional, la seguridad pública, la prevención delictiva, el orden público, la protección de la salud o moral y de los derechos y libertades de otras personas. Por tanto, quedan estrictamente limitados los casos en los que la autoridad pública europea puede quebrantar los derechos relativos a la intimidad, el honor y la propia imagen.

En 1978, la Corte Europea de Derechos Humanos asumió que aunque la sección octava del Convenio no hace mención de las conversaciones telefónicas, éstas si forman parte a efectos del concepto de “intimidad” y “correspondencia”, por tanto, gozan de la misma protección.

La legislación francesa establece sobre la confidencialidad de la correspondencia transmitida por telecomunicaciones, que los casos en los que las autoridades públicas pueden grabar el contenido de la información transmitida, o rastrear el marcado de los números telefónicos deben estar estipulados. De esta forma la Ley limita la violación de los derechos de confidencialidad a casos de necesidad justificada por cuestiones de interés público. De manera que, sólo es posible en el contexto de una petición legal y que sólo se autoriza en caso de una

ofensa suficientemente seria fundamentada en una de las bases legales de interpretación enumeradas en la sección tercera de la Ley, como pueda ser la prevención del terrorismo.

De forma similar encontramos la redacción de la *Interception of Communications Act* inglesa de 1985, que permite la interceptación por razones de seguridad nacional o de prevención y detección de delitos que sean lo suficientemente graves.

La situación en cuanto a la garantía de la confidencialidad entre particulares es más extrema, porque en este caso son las sanciones penales las que se aplican para castigar las violaciones al derecho a la intimidad.

En la legislación de EEUU, la ECPA castiga con multa o cárcel a quien intencionadamente intercepte o lo intente, cualquier tipo de comunicación electrónica interestatal. Esta sanción se refiere al mal uso y acceso a comunicaciones que circulan en Internet.

Estas regulaciones no impiden que los operadores de sistemas cumplan su misión por las siguientes razones:

\* El alcance de la prohibición de interceptación esta actualmente en debate y algunos juristas sugieren que se aplique sólo al acceso en tiempo real por el operador del sistema, no al uso de un archivo que ya se transmitió por Internet y ahora esta almacenado en un ordenador.

\* La Ley sobre confidencialidad de comunicaciones por sí misma proporciona a los operadores de sistemas excepciones frecuentes a la prohibición, que permiten la verificación de control mecánico o de calidad.

En EEUU, encontramos el derecho a la intimidad en el derecho consuetudinario, fuera de su reconocimiento constitucional, y de acuerdo con este agravio al derecho común se entiende que “cualquiera que invada intencionadamente, física o de cualquier otra forma, el aislamiento o reclusión de otro, en lo que se refiere a sus asuntos privados, queda sujeto a la responsabilidad por invasión de la intimidad”. Si tenemos en cuenta que este agravio se aplica a un lugar privado, se puede deducir su aplicación a los archivos informáticos guardados en un lugar privado. En este sentido, la jurisprudencia que ya ha aplicado este agravio a las escuchas telefónicas, y a la interceptación de correo personal, autoriza esta amplia interpretación.

En internet cualquiera que cometa una intrusión ofensiva, puede quedar obligado a compensar a la víctima que hubiera sufrido la invasión de su intimidad.

En el ámbito europeo, encontramos que en la legislación francesa la protección en Internet de la confidencialidad de archivos y expedientes está garantizada por varias leyes. Así, la sección 25 de la ley de 10 de julio de 1991 sobre confidencialidad de la correspondencia a través de servicios de telecomunicaciones, prevé sanciones contra cualquier operador público, operador de red o proveedor de servicio de telecomunicaciones que viole la confidencialidad de la correspondencia confiada al servicio en el que se participa, aún cuando el contenido de tal correspondencia no fuera ni divulgado ni usado.

El Código penal francés introdujo a través de la ley de 5 de enero de 1988, la penalización de cualquiera que intencionadamente y sin respeto a los derechos de terceros, directa o indirectamente introduzca datos en un sistema informatizado, elimine, modifique, procese o transmita los datos allí contenidos. Esta misma ley castiga el fraude perpetrado por una red de telecomunicaciones.

La excepción en la legislación francesa se da en favor de los proveedores de servicio si su acto se justifica por necesidades técnicas.

En el ámbito legal inglés la medida básica referente a la interceptación de información es el *Interception of Communications Act* de 1985, que sanciona penalmente a cualquier persona que intercepte una comunicación durante su transmisión por correo o a través del servicio de telecomunicaciones.

En cuanto al procesamiento de datos personales como forma de amenaza sería al derecho a la intimidad, se ha exigido que la mayoría de los Estados de la Unión Europea y de EEUU, respondan a estos desarrollos estableciendo marcos con condiciones que regulan la creación de tales archivos. Sí bien, se ha entendido que no debe prohibirse de forma total el uso de datos personales para conciliarse así con el derecho a la información, derivado del principio de libertad de expresión fundamental en los Estados sociales y democráticos de derecho.

En EEUU y Canadá sólo existe norma escrita para el procesamiento de datos en el sector público, en el privado se da la autorregulación. En la Unión Europea, la protección legal rige a ambos sectores.

Derivadas de la legislación o de la autorregulación, estas normas son de gran interés para Internet, pues confieren derechos a los usuarios y cibernautas limitando las actividades en la red de ciertos tipos de empresas, como las dedicadas al telemercado, o a la creación de perfiles de consumidores o candidatos.

Los proveedores de servicios, administradores de grupos de interés, y servidores Web, que mantengan archivos de datos personales, están obligados a cumplir las reglas, que como en el caso español, prescribe la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales, (LORTAD). En nuestro caso se debe comunicar la existencia de bancos de datos con información personal a la Agencia de Protección de Datos, a través de la inscripción obligatoria de estas bases de datos en el Registro de la Agencia.

Es necesaria la autorización expresa de los titulares de la información, y los datos no se pueden utilizar para una finalidad distinta a la que se haya autorizado, así mismo, no pueden transmitirse a terceros sin el consentimiento expreso del titular.

En el ámbito europeo, la mayoría de los Estados cuentan con regulaciones sobre protección de datos, que deben adaptarse si es necesario al ordenamiento europeo sobre la protección de las personas físicas respecto a la protección de sus datos personales y de la libre circulación de éstos, que fue adoptado conjuntamente por el Parlamento y el Comité el 24 de octubre de 1995.

La aplicación de este ordenamiento europeo protege la creación de archivos usando datos recopilados mediante Internet, la transferencia de archivos de datos personales por Internet, y la agrupación e interconexión de tales archivos esparcidos por medio de diferentes ordenadores conectados a Internet.

Por dato personal se entiende toda información concerniente a una persona física, identificada directa o indirectamente, también se aplica la norma a las imágenes y sonidos digitalizadas.

La norma define el procesamiento, como cualquier operación o serie de operaciones realizadas y aplicadas a los datos personales, así, la recolección, grabación, organización, almacenamiento, adaptación, extracción, consulta, uso, comunicación o transmisión, radiodifusión o cualquier otro medio de provisión de datos, correspondencia o interconexión, el borrado y la destrucción de los datos.

De esta forma, la solicitud de información en Internet, la consulta de archivos de datos personales, el intercambio de mensajes en grupos de interés, y una gran cantidad de operaciones pueden considerarse procesamiento en la red.

En los países de la Unión Europea se garantiza a los titulares de la información, el derecho de acceso, conocer la identidad del responsable del fichero, el uso que se dará a los datos procesados, y el derecho a corregir la información que esté incompleta o incorrecta.

En Internet cuando se transmite un mensaje que contiene datos personales, es el emisor y no la parte que ofrece el servicio, el responsable del procesamiento. El proveedor del servicio es responsable del proceso adicional, necesario para cumplir su labor.

En cuanto a la transferencia internacional de datos personales en Internet, se plantea un problema crítico, pues la exportación instantánea de los datos a través de la red de un país donde la intimidad este bien protegida, a otro donde lo este menos y desde donde pueda difundirse ilegalmente por el resto del mundo, supone la pérdida de las garantías de respeto del derecho a la intimidad como derecho fundamental.

Existen dos textos internacionales que ofrecen soluciones a este problema, por un lado, la Directivas que rigen la protección de la intimidad y los flujos y exportación de los datos personales de la OCDE, que reconocen el principio de equivalencia, de manera que un Estado miembro de la OCDE puede oponerse a la transmisión de datos personales a otro Estado miembro sí este no ofrece una protección equivalente. No obstante, las Directivas especifican que los países miembros puede establecer esta equivalencia por medio de la autorregulación.

En el ordenamiento europeo se acepta el principio de la transferencia de datos personales a un tercer país, suponiendo que éste garantice un nivel adecuado de protección. Para determinar el nivel de protección se toma en cuenta la naturaleza de los datos, el propósito y duración del proceso, el país de origen y el destino final, las reglas generales o sectoriales vigentes en el tercer país y la seguridad de las medidas observadas.

Podemos concluir, diciendo que el problema no queda solucionado, sino que por el contrario se nos plantean muchas dudas respecto a la validez de las transferencias internacionales de datos personales que se dan en Internet en la actualidad, en cuanto al respeto del derecho a la intimidad, teniendo en cuenta que

la frecuencia en la transferencia internacional de datos personales se esta intensificando de forma exponencial con el desarrollo de la red de redes.