PROTECCIÓN DEL DERECHO A LA INTIMIDAD Y USO DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN

DRA. CINTA CASTILLO JIMENEZ
Profesora de Derecho Informático
Universidad de Sevilla
mc.castillo@parlamento-and.es

PALABRAS CLAVE: Intimidad • Internet • Informatica: Privacidad
KEY WORDS: Privacy • Internet • Computer Science

1. INTRODUCCIÓN

En el ámbito del respeto a los Derechos y libertades de las personas y el uso de las nuevas tecnologías de la información, comenzaremos examinando sumariamente la realidad del fenómeno informático.

Podemos destacar el hecho de que por el proceso de tratamiento de la información, se hace referencia a todos aquellos procesos en cuyo transcurso la existencia, las relaciones geográficas, temporales o lógicas de las informaciones se ven sujetas a transformaciones.

La particularidad del tratamiento automatizado de la información radica en que los procesos a los que sometemos a ésta, hasta hace poco tiempo eran tarea exclusiva de los seres humanos, y ahora los ordenadores, es decir los sistemas electrónicos tienen la capacidad de reproducir o simular las formas de trabajo propias de la mente humana.

Quizás el aspecto en el que más se percibe el enorme progreso en las nuevas tecnologías sea, la velocidad de proceso, la exactitud y la fiabilidad, referida claro esta, a la información tal y como sea facilitada.

La incidencia del desarrollo de las nuevas tecnologías en la sociedad ha sido tan importante, que se prevé que en los próximos años, en la mayoría de los países, más de la mitad de la población activa tendrá una ocupación que de una u otra forma dependerá de la informática. Hoy por hoy el ordenador es un instrumento que nos envuelve, pocas cosas existen en la actualidad que no tengan tras de sí un ordenador.

El impacto de las tecnologías de la información y la comunicación en nuestra sociedad contemporánea merece ser estudiado en distintos ámbitos, como es el de la sociología, la economía o el

derecho, en este sentido se ha producido una auténtica revolución en el régimen jurídico internacional relativo a las transmisiones internacionales de datos personales.

Con la celebración de la Conferencia Internacional de Derechos Humanos en 1968, que organizó Naciones Unidas en Teherán, para conmemorar el XX aniversario de la Declaración Universal de Derechos Humanos, se inició el debate sobre la incidencia del uso de la electrónica en los derechos individuales, discutiéndose, ya entonces, cuáles eran los límites que una sociedad democrática debía establecer para proteger dichos derechos[1] .

Los avances más espectaculares en telemática han facilitado la rapidez en el procesamiento, almacenamiento y distribución de datos personales a escala internacional, llegando a crear un mercado internacional de tratamiento de datos.

2. PELIGROS DERIVADOS DEL USO DE LAS NUEVAS TECNOLOGÍAS

Una vez asumida la realidad del fenómeno informático, presente en cualquier ámbito del quehacer humano, analizaremos los principales peligros que del mismo se derivan, centrándonos en la protección de los derechos fundamentales en relación con las personas y el uso de las nuevas tecnologías de la información.

Así, podemos hablar en primer lugar de los peligros en relación a los derechos de la personalidad del individuo, fundamentalmente los ataques a su intimidad personal. En segundo lugar, los peligros relativos al sistema de garantías y contrapesos que caracteriza a la organización del Estado de Derecho.

En 1968, por primera vez Naciones Unidas dicta una Resolución en torno a los peligros que pueden derivarse del uso de las nuevas tecnologías y la protección de los derechos fundamentales, como el honor y la intimidad. La Asamblea Parlamentaria recomendó al Consejo de Ministros estudiar los peligros que el uso de los equipos tecnológicos y científicos representaba para los derechos humanos.

De todos los aspectos nos centraremos en los peligros puestos de manifiesto y relacionados directamente con los bancos de datos que contienen información personal, sobre todo su uso a través de las redes telemáticas, porque afectan de forma más visible a los Derechos Humanos en lo que se refiere al Derecho al honor y la intimidad personal.

2.1. Peligros relacionados con los derechos fundamentales

Por un lado, existen peligros directos para los derechos y libertades individuales, y por otro, las nuevas formas de ataque hacia el sistema de organización política, el Estado de Derecho, que tiene como misión primordial la garantía de esos derechos y libertades, los dos tipos de peligros tienen

[1] O. Estadella Yuste, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995, p. 13.

como nota común el provenir de la misma fuente, bancos de datos estructurados combinados con potentes sistemas de comunicación[2].

Hasta ahora los bancos de datos se estructuraban de forma manual, o semi-mecanizada, en soporte papel, la transmisión se hacía por medios tradicionales, todo esto ha cambiado para encargarse las nuevas tecnologías de la información de almacenar, gestionar, transformar y reproducir la información de cualquier tipo a una velocidad de vértigo, a través de las telecomunicaciones, siendo hoy un hecho cotidiano[3].

Todo el proceso de informatización ha producido una serie de transformaciones tanto en la estructura social como en los comportamientos individuales, cuyo alcance final aún no podemos definir. Se han producido consecuencias de la racionalización, como son el hecho de que las máquinas desplacen a las personas de sus puestos de trabajo, el conocido desempleo estructural[4].

También podemos hablar de los efectos de las nuevas tecnologías como instrumentos distintos a los descubiertos hasta ahora, que almacenan, planifican, regulan, controlan y transmiten la información, en este sentido se han producido consecuencias que afectan a los ciudadanos y sus opiniones, convirtiéndose en algo dirigible con la ayuda de los sistemas de información, estos sistemas permiten un control exhaustivo sobre las personas.

En este punto, podríamos hacer una reflexión sobre los ataques a la privacidad, refiriéndonos al acopio de informaciones singulares que forman parte de la intimidad de las personas, pero que no plantean riesgo de ataque a ésta por si solas. El problema de indefensión y violación de la conocida ya como privacidad del individuo se produce cuando se combinan estas informaciones aparentemente inocuas, para sacar conclusiones a partir de este precipitado, que inciden directamente en el individuo.

Nos referimos a informaciones tales como las enfermedades sufridas durante la niñez, los ritmos de trabajo, el uso del dinero de plástico, etc. Las nuevas tecnologías permiten hacer los combinados a los que nos venimos refiriendo y pueden dar un retrato robot del candidato o candidata al puesto de trabajo, con el peligro incluso de que los datos manejados sean erróneos, o aún siendo ciertos, el resultado de su combinación no coincida con la personalidad del demandante.

Puede ponerse en peligro la dignidad humana y sus proyecciones, no sólo la garantía de que la persona no va a ser objeto de ofensas o humillaciones, sino también el aspecto positivo que supone el pleno desarrollo de la personalidad. Los derechos comprendidos en este apartado y recogidos en nuestra Constitución, incluyen los derechos a la intimidad personal y familiar, al honor y a la propia imagen. Estos derechos son inherentes a toda persona e inalienables y concretan el valor de la dignidad humana en el Estado social y democrático de derecho[5].

[2] C. Castillo Jiménez, "Delito cibernético, Protección de la intimidad en Internet", en *Informática y Derecho*, Mérida, 1998, pag. 461 y ss.
[3] C. Castillo Jiménez, *Actas del Congreso internacional sobre Delito informático*, Mérida, 1997.
[4] A. E. Perez Luño (coord.), *Derechos humanos y constitucionalismo ante el tercer milenio*, Marcial Pons, Madrid, 1996, p. 11 ss.
[5] A. E. Perez Luño, *Teoría del Derecho, una concepción de la experiencia jurídica*, Tecnos, Madrid, 1997.

Existen también problemas derivados de la dependencia de la sociedad respecto a los sistemas de información, hasta el punto de que el funcionamiento y la seguridad de la sociedad y el Estado esta en manos de un número extremadamente reducido de personas, haciéndose cada vez más patente el hecho de que la información es poder.

El progreso tecnológico puede ser portador de beneficios o de perjuicios, según como se encauce la voluntad humana, dando origen a nuevas situaciones que han provocado la necesidad de nuevas elecciones y decisiones, a veces angustiosas como en el caso de la ingeniería genética, el progreso no puede considerarse como un bien absoluto al que se sacrifican o subordinan los demás valores. La civilización tecnológica tras la segunda guerra mundial, ha reivindicado a través de la sociedad civil avances decisivos en el plano del reconocimiento y las garantías jurídicas de los derechos humanos en el marco planetario[6].

Existe una característica básica en común, que en su dimensión planetaria no se había dado hasta ahora, nos referimos a que nunca un derecho humano, como alguno de los proclamados por la Asamblea General de Naciones Unidas, había sido recogido en los ordenamientos jurídicos de todos los Estados, como nunca hasta ahora la ciencia había llegado a ser patrimonio de todos los pueblos en sus aplicaciones tecnológicas como en el caso de las telecomunicaciones.

Hoy por hoy, factores como la velocidad, la potencia y la capacidad de almacenamiento de los ordenadores pueden suponer una seria amenaza al derecho a la intimidad y privacidad de las personas, riesgo que se ve aumentado cuando se facilita la comunicación entre terminales separados por miles de kilómetros, y no existiendo ningún impedimento técnico para el tratamiento de los 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.

El concepto de privacidad, las amenazas que sufre, y los medios para lograrla, están cambiando como resultado de nuestra nueva vida basada en el ordenador y en la última década por la existencia de la Red de redes de comunicación.

La privacidad debe ser considerada como uno de los valores humanos fundamentales, que sirve a los ciudadanos para mantenerse libres, el hecho de preservar nuestras experiencias privadas es una labor importante sobre todo a la hora de recoger y utilizar la información .

Si el sector de Internet tarda mucho en aprender a respetar la privacidad, no sólo frenará la adopción del comercio y servicios por la mayoría de la población, sino que puede provocar una oleada de relaciones contra la tecnología.

La privacidad y la seguridad nos llevan a cuestiones sobre confianza y cuestiones muy subjetivas acerca de personas, empresas y proveedores de servicios.

[6] A. Sánchez Bravo, *Internet y la sociedad europea de la información implicaciones para los ciudadanos*, Universidad de Sevilla, 2001,p. 102 y siguientes.

2.2. Peligros relacionados con internet

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, 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 pueden representar una invasión de la esfera privada.

En Internet, se recomienda ampliamente a los usuarios, operadores y proveedores 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 una Web de Internet, el libro del Dr. C. Gubber y Mr. Gonod sobre la historia médica y política del que fue presidente de la República Francesa, Francois Mitterand. El libro titulado "Le grand secret", estuvo disponible en Internet sólo unos días, después de que se prohibiera su venta en librerías, y violando los derechos de autor reconocidos en las Leyes de propiedad intelectual[7].

Con este suceso, se abrió el eterno debate en el que se discute sí el derecho a la intimidad limita la libertad de expresión, respecto a asuntos que pueden considerarse de interés público, reforzándose con el argumento del derecho 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 en este caso. Entre estos dos derechos existe un delicado equilibrio que debe ser valorado caso por caso para decidir en cada momento cual de esas 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 correos electrónicos que contienen información personal susceptible de protección, ya sea referente a autoridades públicas o bien, entre usuarios particulares.

La comunidad empresarial de Internet opera en un entorno con una transparencia poco corriente, y la mayoría de la los pioneros de este sector han actuado con un elevado nivel ético, aunque quizá no con la suficiente atención y sensibilidad hacía la confidencialidad de la información personal privada.

Internet supone un sueño para sus usuarios y una pesadilla para los prácticos del Derecho, por una parte, permite concluir transacciones con empresas y consumidores situados en cualquier lugar del planeta, agiliza la comunicación entre las personas. Representa la libertad mundial de información y de la comunicación; es un sueño hecho realidad.

[7] O. Hance, *Leyes y negocios en Internet*, Mcgraw-Hill, México, 1996, p.39 y siguientes.

Por otro lado, todo conjunto de actividades sociales precisa una regulación, las legislaciones nacionales avanzan con mucho retraso con respecto a las nuevas tecnologías, esto hace difícil las respuestas legales a los numerosos litigios que pueden suscitar las operaciones en Internet. Por eso es también una pesadilla jurídica.

Un usuario de Internet español y residente en nuestro país, puede acceder a la red y contactar con una empresa alemana vendedora o prestadora de servicios, gracias al acceso a Internet proporcionado por la filial holandesa de un proveedor norteamericano. Las fronteras estatales se diluyen en Internet, la aldea global se ha hecho realidad.

Podemos decir que las cuestiones legales más espinosas que plantea el ciberespacio corresponde al Derecho internacional privado.

2.3. Recorrido por las legislaciones en torno a Internet

La legislación europea y americana hacen distinción según se trate de autoridades públicas o privadas. En la legislación de EEUU y Canadá la protección de la intimidad en la esfera pública esta garantizada como derecho constitucional de aplicación a las comunicaciones electrónicas y por tanto, a Internet. Esta protección constitucional se aplica a los órganos gubernamentales[8].

Las leyes que protegen el derecho a la intimidad en este ámbito en EEUU (Electronic Communications Privacy Act) y en Canadá (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 que lo permita.

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 dado. Con la aplicación de estas medidas en Internet las autoridades no necesitan 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 se da desde las distintas Constituciones y las normas de desarrollo de éstas dedicadas a la protección del derecho a la intimidad, así como el Convenio europeo de derechos humanos[9].

Este Convenio limita las medidas adoptadas por las leyes nacionales de los Estados firmantes para permitir el acceso a las comunicaciones en general, y las transmisiones en Internet en particular, por parte de las autoridades gubernamentales[10].

La sección octava del Convenio garantiza el derecho a la intimidad y confidencialidad de la correspondencia, esto supone que las autoridades deben garantizar el respeto a la intimidad entre los ciudadanos, y así mismo abstenerse de toda interferencia, a menos que se den circunstancias excepcionales que deben estar previstas por Ley. Esta interferencia debe ser necesaria y proporcionada

[8] M. A. Davara Rodríguez, *La protección de los datos en Europa*, ICAI-ICADE, Madrid, 1998.

[9] M. Heredero Higueras, *La Directiva Comunitaria de protección de datos de carácter personal*, Aranzadi, Madrid, 1997.

[10] Mª Luisa Fernández Esteban, "La regulación de la libertad de expresión en Internet, en EEUU y en la Unión Europea", *Revista De Estudios Políticos*, nº 103, 1999.

dentro de las normas de una sociedad democrática, y tener como objeto la seguridad nacional, el orden público, la prevención delictiva, la protección de la salud, de los derechos y libertades de las personas. De esta forma, quedan 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 alusión a las conversaciones telefónicas, éstas si forman parte y gozan de la misma protección a los efectos del derecho de intimidad y lo que se entiende por correspondencia.

La legislación francesa en lo que se refiere a la confidencialidad de la correspondencia transmitida a través de las telecomunicaciones establece, 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 ser estipulados. De esta forma, la Ley limita la violación de los derechos de confidencialidad a casos de necesidad justificada por cuestiones de interés público. Por tanto, sólo es posible en el contexto de una petición legal y 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 puede ser la prevención del terrorismo.

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

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, por distintas razones: por un lado, el alcance de la prohibición de intercepción 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. Por otro, la Ley sobre confidencialidad de comunicaciones por sí misma proporciona a los operadores de sistema excepciones frecuentes a la prohibición, que permitan la verificación de control mecánico o de calidad.

En EEUU, el Derecho a la intimidad se encuentra en el Derecho consuetudinario, fuera del reconocimiento constitucional, así se entiende que "cualquiera que invada intencionadamente, física o de cualquier otra forma el aislamiento de otro, en lo que se refiere a sus asuntos privados, queda sujeto a la responsabilidad por invasión de la intimidad". Teniendo 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, así la jurisprudencia aplicada a las escuchas telefónicas, y a la intercepción del correo personal, autoriza esta amplia interpretación.

En Internet cualquiera que cometa una intrusión ofensiva, puede quedar obligado a compensar a la víctima de la invasión de su intimidad[11].

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, 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 divulgado ni usado.

El Código penal francés introdujo en 1988 a través de la Ley de 5 de enero, 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 en una red de telecomunicaciones.

La excepción en la legislación francesa se da a 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 interpretación 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 de las telecomunicaciones.

En cuanto al procesamiento de datos personales como forma de amenaza seria al derecho a la intimidad, se ha exigido que los Estados de la Unión Europea y de EEUU, respondan a estos desarrollos estableciendo marcos con condiciones que regulen la creación de tales archivos, sin prohibirse de forma total el uso de datos personales, de manera que pueda garantizarse 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.

En Internet, los proveedores de servicios, administradores de grupos de interés, y servidores Web, que mantienen archivos de datos personales están obligados a cumplir las reglas. En España la Ley 15/99 de protección de datos de carácter personal que sustituyó a la LORTAD, exige la inscripción obligatoria de las bases de datos con información personal en el Registro de la Agencia de Protección de Datos. Se requiere 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 sin el consentimiento expreso de su titular.

En el ámbito europeo, la mayoría de los Estados cuentan con regulaciones sobre protección de datos, adaptadas al ordenamiento europeo sobre la protección de las personas físicas respecto a la

[11] E. Moron Lerma, *Internet y derecho penal, hacking y otras conductas ilícitas en la red*, Aranzadi, 1999, p. 46 ss.

protección de sus datos personales y de la libre circulación de éstos, según acordó el Parlamento y el Comité el 24 de octubre de 1995.

La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos[12], creó el Grupo de Trabajo sobre protección de las personas, este grupo tiene la obligación de facilitar a la Comisión, al Parlamento Europeo y al Consejo un informe anual sobre el estado de protección de las personas físicas con respecto al tratamiento de los datos de carácter personal en la Comunidad y en terceros países[13]. El grupo se compone de representantes de las autoridades nacionales independientes encargadas de la protección de datos y un representante de la Comisión.

Una de las funciones principales del Grupo de Trabajo es la de formular dictámenes sobre el nivel de protección en la Unión y en los terceros países, y emitir recomendaciones sobre cualquier cuestión referente a la protección de las personas con respecto al tratamiento de los datos personales.

Tomando la Directiva como punto de partida y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos, debemos referirnos a un núcleo de principios de contenido de protección de datos y requisitos de procedimiento y de aplicación cuyo cumplimiento debe considerarse un requisito mínimo para juzgar la adecuada protección. El grado de riesgo para el interesado, en caso de transferencia internacional supone un factor importante para determinar los requisitos concretos en un caso determinado.

2.4. Principios de la protección de los datos personales

Los principios fundamentales de la protección de las personas a través de sus datos personales son:

Principio de limitación de objetivos, finalidad. Los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia.

Principio de proporcionalidad y de calidad. Los datos deben ser exactos y estar actualizados, deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

Principio de transparencia, información en la recogida de los datos. Debe informarse a los interesados sobre el objetivo del tratamiento y de la identidad del responsable en el tercer país.

Principio de seguridad. El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos.

La aplicación del ordenamiento europeo protege la creación de archivos usando datos recopilados a través de Internet, la trasferencia a través de la red y la agrupación e interconexión de tales archivos conectados a través de ella. Entendiéndose por dato personal toda información concer-

[12] M. Heredero Higueras, *La Directiva comunitaria de protección de datos de carácter personal*, Aranzadi, Madrid, 1997.
[13] O. Estadella Yuste, *La protección de la intimidad...*

niente a una persona física, identificada directa o indirectamente, así como a las imágenes y sonidos digitalizados.

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

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 son consideradas como procesamiento en red.

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

Cuando se transmite un mensaje que contiene datos personales, a través de Internet 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.

2.5. Regulación de los problemas planteados en Internet

La transferencia internacional de datos personales plantea un problema crítico, ya que la exportación instantánea de los datos en la red de un país con protección del derecho a la intimidad, a otro con una protección menor y desde donde puede difundirse ilegalmente por el resto del mundo, supone la pérdida de las garantías de respeto del derecho fundamental a la intimidad. Hay textos internacionales que ofrecen soluciones a este problema, por un lado, las Directivas que rigen la protección de la intimidad y los flujos de información personal de la OCDE (Organización para la Cooperación y el Desarrollo Económico), que reconocen el principio de equivalencia de manera que un Estado miembro puede oponerse a la transmisión de datos personales a otro que no ofrezca una protección equivalente. Por otro lado las Directivas especifican que los países miembros pueden establecer esta equivalencia por medio de la autorregulación[14].

De esta forma, en términos generales el ordenamiento europeo acepta el principio de transferencia de datos personales a un tercer país sí este garantiza un nivel adecuado de protección. Para determinar el nivel de protección se toma en cuenta la naturaleza de los datos, el objeto y duración del proceso, las normas generales o sectoriales vigentes en el país y la seguridad de las medidas observadas[15].

Es importante por tanto, definir el concepto de IPI, como información personalmente identificable. Se hace referencia a todo lo que en la red electrónica puede ser vinculado o relacionado con una persona, y por ello con su privacidad, dignidad y libertad[16].

[14] S. Muñoz Machado, *La regulación de la red, poder y derecho en Internet*, Taurus, Madrid, 2000,p.151.
[15] AA.VV., *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001, p. 153 ss.
[16] AA.VV., *La centésima ventana*, Deusto, Bilbao, 2000, p. 197 ss.

La actuación del Grupo de Trabajo en relación con Internet, dada la penetración de la red en todos los ámbitos de la sociedad de la información, estimó la conveniencia en 1999 de formar un subgrupo especializado, con miembros de las distintas autoridades de control provenientes tanto del campo del Derecho como de las Tecnologías de la Información para proceder a un estudio sistemático de aquellos temas o categorías de tratamientos en Internet que tienen mayor incidencia sobre la intimidad de las personas.

En la sociedad de la información en la que vivimos inmersos, el ciudadano debe ser el centro de toda la actividad, primándose la protección de sus derechos, lo contrario sería llevar a los procesos tecnológicos a una despersonalización que la vaciaría de contenido.

El flujo de informaciones entre los distintos países europeos es un instrumento indispensable de conocimiento, pero tiene que ser también a través de la protección jurídica adecuada, la base sobre la que fomentar el respeto mutuo, la tolerancia y la consecución de metas comunes.

Las tecnologías de la información y la comunicación pueden servir igual para aumentar las diferencias entre unos y otros, o bien para integrarnos en el mutuo conocimiento con el respeto imprescindible a los derechos y libertades fundamentales.

La Unión Europea responde de forma inmediata a este fenómeno que tiene una dimensión planetaria, y tiene en la autorregulación y en la concienciación de los usuarios la verdadera clave de la eficacia.

Podemos apuntar algunas conclusiones que se plasman en los distintos documentos adoptados por el Grupo Operativo de Internet. Por un lado no podemos hablar de un vacío legal, pues tanto la Directiva 95/46/CE y la 97/66/CE, como las leyes nacionales aprobadas a consecuencia de la trasposición de las mismas, son aplicables a Internet, lo que implica que tanto los principios de protección de datos como los derechos de los ciudadanos en relación con la protección de sus datos personales son exigibles cuando los tratamientos se realizan en Internet.

Hay que informar explícitamente al usuario de Internet de qué datos se le están recabando, ya sea de forma explícita o implícita, dándole la oportunidad de oponerse al tratamiento de los mismos[17].

Por último, los datos no deben conservarse a efectos exclusivos de control de cumplimiento de la ley por los operadores de telecomunicaciones, proveedores de servicios de Internet, no debiendo establecerse obligaciones legales sobre la conservación de estos datos durante un plazo superior al necesario para cubrir las necesidades sobre reclamaciones.

El panorama político mundial excluye cualquier solución legislativa duradera y válida para regular esta situación, por las características de Internet, que salta fronteras, legislaciones y sistemas punitivos se hace imprescindible el consenso internacional para regular este fenómeno y luchar contra los contenidos indeseables, a partir de ese consenso se podrá abordar la regulación jurídica de la red, hasta ese momento habrá que propiciar desde dentro y fuera de la red las normas de buena conducta o códigos deontológico.

[17] P. Llaneza Gonzalez, *Internet y comunicaciones digitales*, Bosch, Barcelona, 2000, p. 259 ss.

Ni las conferencias anuales de las autoridades nacionales de protección de datos, ni el Comité consultivo del Convenio 108, han aspirado a convertirse en una autoridad supranacional, pero sin duda su instauración permitiría aumentar la libre circulación de la información sin que la intimidad individual se viera perjudicada.

El ámbito de actuación de esta autoridad debería ser internacional, e incluirse en el marco de la ONU, esto puede ser demasiado ambicioso teniendo en cuenta la falta de experiencia y tradición legal de muchos países no europeos en el tema de protección de datos. Por tanto, sería más efectivo que antes de instaurar una autoridad cuasiuniversal, todos los países incorporasen a sus legislaciones nacionales los principios y directrices de la ONU y los cumplan.

En el marco europeo el Consejo de Europa sería el competente para crear esa autoridad, sobre todo, por la experiencia de los últimos treinta años en el tema de protección de datos.

En el tránsito de los antiguos derechos naturales a los nuevos derechos humanos se ha evidenciado un cambio de perspectiva total, de los derechos racionales invocados por la filosofía que han dado paso a los derechos positivos incorporados a las leyes estatales y a los tratados internacionales[18].

Los derechos ligados al estatus del ciudadano han ampliado su ámbito de referencia a las formaciones sociales, de los derechos comprendidos en un catálogo cerrado y ahistórico se ha pasado a una concepción abierta y progresiva de los mismos para adecuarla a las nuevas necesidades del hombre creador del mundo tecnológico.

La seguridad efectiva y práctica de la información gestionada electrónicamente es un interés incuestionable, su tutela debe asegurarse sin comprometer los intereses de la población en general. Las medidas restrictivas de derechos que deban ser adoptadas para la prevención y represión de los ilícitos perpetrados en Internet, deben ser, justificadas, necesarias y proporcionales.

Por ello, no debe aceptarse la aplicación analógica a Internet de normativa reguladora de otros medios, y por tanto, de realidades distintas a la de las redes telemáticas de información, por que ello podría suponer la cercenación de principios fundamentales como el de legalidad y el de proporcionalidad[19].

Existen dos grandes corrientes de pensamiento en torno a la regulación de los litigios surgidos en Internet. Por un lado, la elaboración de una normativa especialmente diseñada para Internet[20].

Esta norma puede adoptar formas diferentes; códigos de conducta de los internautas, autorregulaciones de los proveedores de acceso a Internet, usos, principios básicos adoptados por asociaciones profesionales u organizaciones internacionales.

La otra opción, consiste en regular los conflictos legales que plantea Internet mediante las tradicionales reglas estatales de competencia judicial internacional, es decir lo que señalan los Tribunales estatales competentes para conocer de supuestos internacionales.

[18] A. Sánchez Bravo, *Internet...*
[19] E. Moron Lerma, *Internet y Derecho penal...*
[20] AA.VV., *Conflictos de Leyes...*

Estaríamos ante las conocidas reglas sobre efectos de decisiones extranjeras, que determinan la posibilidad de que decisiones públicas emanadas por autoridades de un país sean efectivas en otros países.

Esta segunda opción supone la aplicación del Derecho internacional privado, a lo que añadimos que debe construirse un Derecho internacional privado para Internet, de manera que el operador jurídico debe hacer justicia en las situaciones privadas internacionales, debiendo forjar una solución nueva mediante un desarrollo judicial del Derecho internacional privado basado en valores constitucionales.

En este sentido, el tratamiento de los datos personales en Internet depende en su aplicación del Derecho internacional privado, de que se trate de un país de la U.E. o no, por tanto las empresas deben tener en cuenta la pluralidad de leyes nacionales, de forma que las empresas no pueden recibir libremente datos personales desde la U.E. a menos que el país donde radiquen tenga un nivel de protección adecuado.

Para determinar cuándo un país goza de un nivel de protección adecuado de la intimidad frente al uso de la informática, es una cuestión problemática que plantea dificultades entre USA y la UE. En USA no hay regulación estatal sobre esta materia, las compañías se autorregulan mediante códigos de conducta, esto ha provocado que la Comisión de la UE, prohibiera en 1998 la transmisión de datos desde la UE a USA a la espera de negociar un acuerdo. A su vez, USA acusa a la UE de erigir obstáculos a los intercambios comerciales.

3. Conclusiones.

Para terminar, daremos algunas conclusiones sobre el análisis de la tecnología informática y las modernas redes globales, y el efecto que pueden tener sobre la seguridad y privacidad personal.

La evolución de Internet ha producido un paso del escenario electrónico de libre expresión y una interacción no comercial a convertirse en una sofisticada plataforma de marketing y entretenimiento que está impulsada en gran parte por el comercio electrónico.

La importancia comercial de los sistemas informáticos en red ha dado lugar a innovaciones y adelantos en la recogida, almacenaje y distribución de información personal identificable (IPI), los recolectores de datos utilizan los últimos avances técnicos para conocer los gustos, valores y formas de conducta de las personas.

La sofisticación de los medios de recogida y distribución de la IPI, resulta preocupante por la vulnerabilidad de los sistemas, de manera, que es más fácil recoger y distribuir IPI que garantizar su confidencialidad.

El derecho a la intimidad y concretamente la privacidad son requisitos fundamentales para una sociedad libre que a través de Internet están siendo atacados.

Los gobiernos no sólo no están preparados para combatir la erosión de la privacidad en la era Internet, sino que a menudo son los primeros que la llevan a cabo.

En nuestros días no es fácil determinar la fiabilidad de las empresas que recogen y utilizan la IPI y por ello, es más difícil frenar la proliferación y profundidad de los perfiles existentes en la red

sobre cada uno de nosotros, y serán más abundantes las brechas de seguridad, los nuevos derrumbes de la privacidad, los nuevos métodos que ocultamente manejan la identidad personal detrás de la cortina electrónica. Las personas que se preocupan por mantener un poco de anonimato personal llegan a la conclusión de que la privacidad ya es menos un derecho, y más una capacidad y una técnica.

Para terminar, y en resumen decir que Internet esta pasando por una importante transición impulsada por una nueva necesidad de equilibrar lo público y lo privado, así como los valores humanos y la eficacia técnica. Creemos que el resultado de esta transición, en último término, será el nacimiento de una nueva arquitectura en red basada en dos valores fundamentales: la transparencia y la confianza[21].

RESUMEN: Con estas notas hemos querido contribuir a las aportaciones que consideramos de máxima actualidad, sobre las implicaciones de las nuevas tecnologías de la información y la comunicación y el respeto de los derechos fundamentales como son el honor y la intimidad personal.

Hemos recorrido las influencias del uso de la ciencia informática en nuestros días y nos hemos detenido en los peligros que ese uso plantea para la garantía de los derechos fundamentales.

Después de hacer una reflexión histórica y de derecho comparado, del camino seguido por los distintos países en cuanto a la regulación y la protección de los datos personales, nos hemos detenido en el glosario de principios que garantizan esa protección de las personas en cuanto a sus datos, fundamentalmente en Europa y EEUU.

También hemos querido aportar nuestra opinión sobre la construcción del concepto de privacidad, y como se transforma con la aplicación de las nuevas tecnologías. Hemos analizado la situación actual en cuanto a protección y garantías de derechos en Internet, y como se presenta el futuro inmediato en la red de redes, en lo que se refiere el respeto de la intimidad y la privacidad.

Por último, hemos concretado algunas de las ideas que consideramos válidas para solucionar los problemas puestos de manifiesto por el conflicto suscitado entre el sueño que supone el uso de las nuevas tecnologías de la información y la comunicación, y la pesadilla jurídica planteada por las respuestas legales necesarias ante los numerosos litigios planteados en Internet.

ABSTRACT: With these notes we have tried to contribute to the ideas we consider highly important current issue about contradictions between new Information and Communication Technologies and the respect for basic rights as honour and personal privacy. We have surveyed the influence of the use of Computer Science nowadays and paid attention to the risks this use raises for basic rights safeguard. After a historical and comparative Laws reflection about the way other countries have regulated private data protection, we have especially checked the glossary of principles that guarantee that personal information safeguard, mainly in Europe and USA. We also give our opinion about the construction of the concept of privacy and the way it is modified in applying new Technologies. We have analized the present-day situation with regard to protection and rights safeguards in Internet and how the near future comes up in the network referring to respect to privacy and intimacy. Finally we have specified some of the ideas we consider valuable to solve the problem shown by the clash between the dream of using the new Information and Communication Technologies and the juridical nightmare raised for the necessary legal responses faced to so many lawsuits raised in Internet.

[21] P. Llaneza González, Internet y comunicaciones digitales, Bosch, Barcelona, 2000, p.259 y siguientes.