

LA SOCIEDAD DE LA INFORMACIÓN Y LOS DERECHOS FUNDAMENTALES. LEY 34/2002 DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DEL COMERCIO ELECTRÓNICO

CINTA CASTILLO JIMÉNEZ

Profesora de Filosofía del Derecho y Derecho informático
Universidad de Sevilla

ÍNDICE: 1. Introducción. 2. El derecho a la intimidad y la sociedad de la información. 2.1. La libertad en la sociedad de la información. 2.2. Protección jurídica. 3. La protección de datos personales como derecho fundamental. 3.1. Principios que rigen la protección de las personas a través de sus datos. 3.2. Sentencia 292/2000 de 30 de noviembre, del Tribunal Constitucional. 4. Regulación a través de la LSSI de los problemas planteados en Internet. 4.1. Panorama mundial. 4.2. Ley 34/2002 de servicios de la sociedad de la información y comercio electrónico. 5. Conclusiones.

INDEX: 1. Introduction. 2. The right to privacy and the information society. 2.1 Freedom in the information society. 2.2. Law safeguard. 3. The private data safeguard as a fundamental right. 3.1. Principles that rule people safeguard with private data. 3.2. Decision 292/2000 of the Constitutional Court. 4. Regulation of problems raised in Internet under the LSSI. 4.1. Mundial assessment. 4.2. “Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico”. 5. Conclusion.

PALABRAS CLAVE: Comercio electrónico • Internet • Informática • Protección de datos • Sociedad de la información

KEY WORDS: Electronic commerce • Internet • Computer Science • Data safeguard • Information society

1. INTRODUCCIÓN

Un año después de la entrada en vigor de la Ley 34/2002 de 11 de julio que regula los Servicios de la Sociedad de la información y el Comercio electrónico y más conocida como la Ley de Internet, estamos en condiciones de analizar su contenido y sobre todo los mecanismos que se establecen para garantizar el respeto de los derechos fundamentales.

Los avances tecnológicos y su implantación en la sociedad actual nos están permitiendo presenciar y ser protagonistas del estallido de una nueva revolución, más fuerte que la revolución industrial y con la enorme diferencia de que si bien aquella fue vivida por unos pocos, esta tiene un carácter universal y es percibida por muchos.

Entre la Ilustración y nuestros días, desde la enciclopedia a la red, se ha ido gestando a una velocidad uniformemente acelerada el progreso científico y su aplicación a todos los ámbitos de la vida.



En un mundo con más de seis mil millones de seres humanos, la globalización o mundialización establece como presupuesto jurídico, por una parte, la ciudadanía común, universal, y por otro un espacio judicial sin fronteras. La globalización es obra de varios factores convergentes entre los que se encuentra la comunicación instantánea y exhaustiva a través de la informática y la telemática. La libertad de comercio y la economía de mercado, también hacen posible la globalización de las necesidades.

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. 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.

La idea de sociedad de la información engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actitudes individuales y formas de organización política y administrativa, de importancia creciente en las naciones situadas en la vanguardia económica y cultural, a la que no pueden ser ajenos los poderes públicos¹.

Los servicios de la Sociedad de la Información pretenden cubrir una amplia variedad de actividades económicas que se desarrollan en línea, bien sea la venta de mercancías, las comunicaciones comerciales o los instrumentos de búsqueda, acceso y recopilación de datos.

No podemos dejar de tener la visión de la Sociedad de la información y de la economía interrelacionadas a nivel mundial, fruto de la globalización, donde las tecnologías de la información y de las comunicaciones desempeñan un papel decisivo en la transformación en todos sus aspectos. La industria de los contenidos es un sector crucial en la sociedad de la información, incidiendo fundamentalmente en el empleo, la competitividad y los aspectos culturales. Siendo los servicios de la sociedad de la información un importante vehículo de la identidad cultural y la diversidad lingüística europea. La libre circulación de información contribuye al desarrollo cultural de los pueblos.

Según la Directiva 2000/31/CE, la sociedad de la información es el resultado de la extraordinaria expansión de las redes de telecomunicaciones, y en especial de Internet, como vehículo de transmisión e intercambio de todo tipo de información.

La implantación de Internet ha producido incertidumbres jurídicas, que ha hecho necesario establecer un marco jurídico adecuado que sirva para generar en todos los actores intervinientes la confianza necesaria para el empleo de la Red.

¹ R.D. 1289/1999, de 23 de julio de Creación de la Comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías.

La Sociedad de la Información en este marco universal genera una serie de actividades que tienen un soporte trascendente en los derechos fundamentales, en el ámbito de la libertad de expresión y el derecho a la información.

El derecho a la intimidad personal y familiar y la protección de los datos personales, el derecho a la imagen, la libertad informática, el derecho de autor y otros instrumentales como la libertad de empresa y la libre competencia en una economía de mercado.

2. EL DERECHO A LA INTIMIDAD Y LA SOCIEDAD DE LA INFORMACIÓN

La información, que siempre ha sido valiosa, en nuestros tiempos se ha convertido en absolutamente necesaria, entre toda cobran especial relevancia los datos de carácter personal.

La dimensión del conocimiento científico plantea una dicotomía entre la conveniencia de saber y el temor de averiguar lo que no gusta. 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 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.

La intimidad, como derecho subjetivo, no consiste tan sólo en impedir la obtención y difusión por cualquiera de datos o circunstancias ajenas, sin el consentimiento del afectado, sino que se convierte en un derecho reaccional frente a la injerencia de los poderes públicos que pretendan imponer coactivamente un estilo de vida o modificar la conducta de los individuos en la sociedad en la que viven. Se puede definir por tanto, como el derecho a ser dejado solo, derecho a la soledad libremente escogida.

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 derecho².

Las legislaciones y la jurisprudencia de los Tribunales de los países de la Unión Europea y de EE.UU., 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.

2.1. LA LIBERTAD EN LA SOCIEDAD DE LA INFORMACIÓN

La prestación de servicios de la Sociedad de la información se rige por el principio de libertad, y por tanto, no está sujeta a autorización previa ni a ningún tipo de restricción por razones derivadas del ámbito normativo, según el Art. 6 de la Ley. Esta norma se ve amparada por la propia Constitución en lo que se refiere a la libertad de expresión y el derecho de información en su doble vertiente.

Los límites se establecen en el Art. 8, como restricciones a la prestación de servicios, entre las que se encuentran la salvaguarda del orden público, la protección de la salud, el respeto a la dignidad de las personas y principio de no discriminación, así como la protección de la juventud y de la infancia.

Las medidas de restricción deben respetar en todo caso, las garantías normas y procedimientos previstos en el ordenamiento jurídico, que protegen los derechos a la intimidad personal y familiar, la protección de datos personales, la libertad de expresión o la libertad de información.

² A. E. Pérez Luño, "Una concepción de la experiencia jurídica", *Teoría del Derecho*, Tecnos, Madrid, 1997.

Para garantizar la efectividad de la interrupción de la prestación del servicio o la retirada de los datos procedentes de un prestador establecido en otro Estado, el órgano competente impedirá el acceso desde España ordenando a los prestadores de servicios de intermediación establecidos en España, directamente o a través de solicitud motivada del Ministerio de Ciencia y Tecnología, que se tomen las medidas necesarias para impedir dicho acceso.

Cuando se establezcan restricciones que afecten a un servicio de la Sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea distinto de España, el órgano competente requiere al Estado miembro en el que este establecido el prestador afectado para que adopte las medidas oportunas, de no hacerse se notificará a la Comisión europea, o al Comité mixto del espacio económico europeo y al Estado miembro para que se traten las medidas que se tienen intención de tomar. Los requisitos y notificaciones se harán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de la información a las Comunidades Europeas.

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.

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.

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.

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.

2.2. PROTECCIÓN JURÍDICA

La regulación de la Sociedad de la Información se hace imprescindible ante la aparición de nuevas actividades y también de nuevos actores e intermediarios.

Como dice el Profesor Pérez Luño “Los juristas debemos realizar un esfuerzo para superar la tendencia congénita a escanciar el vino nuevo de las cuestiones que emergen del cambio social y tecnológico en los odres viejos conceptuales y metódicos de la dogmática jurídica tradicional”³.

La Unión Europea, a través de diferentes recomendaciones, decisiones del Consejo y Directivas, ha tratado desde hace más de una década, armonizar las legislaciones de los diferentes Estados miembros, sobre las materias que inciden en la Sociedad de la Información.

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.

El uso de la Red 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.

La Unión Europea, consciente de la necesidad de proteger a las personas físicas respecto al tratamiento de sus datos de carácter personal y a la libre circulación de éstos ha aprobado las Directivas:

- 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- 97/66/CE del Parlamento Europeo 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 la telecomunicaciones.

³ A. E. Pérez Luño, *Manual de Informática y Derecho*, Ariel Derecho, Barcelona, 1996.

- 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Las dos primeras Directivas han sido incorporadas ya al ordenamiento jurídico español, no habiéndolo sido aún la tercera.

La Directiva 95/46/CE dio origen a la Ley Orgánica 15/99, de protección de datos de carácter personal, que derogó a la LORTAD.

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.

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 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 humano.

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 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 manera 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 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 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 interceptación del correo personal, autoriza esta amplia interpretación.

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 nuestro país, la protección de datos e carácter personal en la transferencia internacional de éstos se regula a través de la Directiva 95/46/CE del Parlamento Europeo en lo que respecta al tratamiento de los datos y la libre circulación de éstos. Por la Ley Orgánica 1571999 de Protección de Datos de Carácter Personal y por la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos⁴.

3. LA PROTECCIÓN DE LOS DATOS PERSONALES COMO DERECHO FUNDAMENTAL

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 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 datos⁵, 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.

⁴ Emilio del Peso Navarro, “Comercio electrónico y protección de datos”, *Servicios de la Sociedad de la Información*, Díaz de Santos, Madrid, 2003.

⁵ M. Heredero Higuera, *La Directiva comunitaria de protección de datos de carácter personal*, Aranzadi, Madrid, 1997.

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.

No podemos perder la visión de la Sociedad de la Información y de la economía interrelacionadas a nivel mundial, fruto de la globalización, donde las tecnologías de la información y de las comunicaciones desempeñan un papel decisivo en la transformación en todos sus aspectos.

Vivimos en el albor de una nueva era, donde el músculo es sustituido por el conocimiento, la presencia física de un objeto por lo intangible y la materialidad por la realidad virtual⁶.

3.1. PRINCIPIOS QUE RIGEN LA PROTECCIÓN DE LAS PERSONAS A TRAVÉS DE SUS DATOS

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

- La finalidad con que se recaban y usan los datos como principio de limitación de objetivos. 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.

- La proporcionalidad y la 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.

- La transparencia en la información, y en la recogida de los datos. Debe informarse a los interesados sobre el objetivo del tratamiento, así como de la identidad del responsable del fichero.

- La seguridad. El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos y establecidas en la Ley.

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

⁶ Domingo Carbajo Vasco, *Informe sobre el impacto del comercio electrónico en la fiscalidad española*.

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

La Ley de la Sociedad de la información define 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.

3.2. SENTENCIA 292/2002 DEL TRIBUNAL CONSTITUCIONAL

A partir de la Sentencia 292/2000 del Tribunal Constitucional, la protección de los datos de carácter personal adquiere en España el carácter de derecho fundamental independiente del derecho a la intimidad.

Esta Sentencia establece que la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede al ámbito propio del derecho fundamental a la intimidad reconocido en el art. 18.1 CE, y que se traduce en el derecho de control sobre los datos relativos a la propia persona.

La libertad informática se traduce en el derecho a controlar el uso de los datos personales insertos en un programa informático, a través del “habeas data” y comprende entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

El derecho fundamental a la protección de datos, atribuye a su titular facultades para imponer a terceros la realización u omisión de determinados comportamientos regulada por Ley que desarrolla los arts. 18.4, 81.1 y 53.1 de la CE.

El derecho a la intimidad como derecho fundamental, protege frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, para impedir su tráfico ilícito y lesivo para su dignidad y derecho como afectado.

En definitiva, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno y el derecho a la protección de datos garantiza a los individuos el poder de disposición sobre sus datos.

Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, así como el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidos de dicha información.

Para que el titular de la información pueda disponer de sus datos, es imprescindible que sepa que datos son los que se conocen, quiénes los poseen y con qué fin.

El derecho a la protección de datos personales es más amplio que el propio derecho a la intimidad, porque si bien, este se extiende a los bienes de la personalidad que pertenecen al ámbito de la vida privada y permite el pleno ejercicio de los derechos de la persona.

El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes en el ejercicio de los derechos de la persona, sean o no derechos constitucionales, por tanto sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado.

El objeto de protección del derecho fundamental a la protección de datos alcanza a los datos personales públicos, es decir todos aquellos que identifiquen o permitan la identificación de su titular, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole que constituya una amenaza para el titular.

Otra peculiaridad del derecho fundamental a la protección de datos es la de atribuir al titular de los datos un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad. Estos deberes jurídicos se materializan en derechos como el de consentimiento del titular, el de información sobre el destino de los datos, el derecho de acceso y el de rectificación y cancelación, en definitiva todos los que garantizan el poder de disposición sobre los datos personales por parte de su titular.

Podemos concluir, que el derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los propios datos personales que faculta a la persona a decidir cuales de estos datos esta dispuesto a proporcionar a un tercero, ya sea el Estado o un particular.

Por tanto, los elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales, son los derechos que garantizan la información, el acceso y el poder oponerse a la posesión y uso.

La autodeterminación informativa nace como la expresión máxima de control sobre los datos personales que puede tener el interesado. Tras la Sentencia del Tribunal Constitucional Alemán de 1983 por la que se declaraba inconstitucional algunos aspecto de la Ley del Censo.

A través del derecho de información y acceso, de rectificación y de cancelación de la información se hace posible el ejercicio de la autodeterminación que no es total, pues no podemos desaparecer de los bancos de datos de las Administraciones a las que nos vemos obligados a prestar nuestros datos personales. Pero que permite en los demás casos controlar que información tienen los demás sobre nosotros y cual queremos que tengan.

Existe un cauce procesal para llevar a cabo la autodeterminación informativa conocido como "Habeas Data", que permite el conocimiento de la información que tienen sobre nosotros y que permite a partir de esa información ejercer el resto de los derechos incluidos en la Ley de Protección de Datos. El instrumento por el que se hace posible el ejerci-

cio de los derechos, es la Agencia de Protección de Datos, a través de la cual se hacen las consultas y las reclamaciones en todo lo que concierne a la protección del derecho fundamental de la intimidad personal.

4. REGULACIÓN A TRAVÉS DE LA LSSI DE LOS PROBLEMAS PLANTEADOS EN INTERNET

4.1. PANORAMA MUNDIAL

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 autorregulación⁷.

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.

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.

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.

⁷ S. Muñoz Machado, *La regulación de la red, poder y derecho en Internet*, Taurus, Madrid, 2000. pgs. 151

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.

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 mismos⁸.

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.

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 cuasi universal, 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 internacionales⁹.

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 pobla-

⁸ P. Llana González, *Internet y comunicaciones digitales*, Bosch, Barcelona, 2000, pgs. 259 y ss.

⁹ A. Sánchez Bravo, *Internet y la sociedad europea de la información: implicaciones para los ciudadanos*, Sevilla, 2001.

ción 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 proporcionalidad¹⁰.

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.

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.

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 UE 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 UE 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, debe compararse el nivel de protección de los datos con el país origen de la información, debiéndose al menos igual el nivel de protección.

En este sentido, surge como una cuestión problemática por las dificultades que se plantean entre el nivel de protección en USA y la Unión europea.

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 Unión europea, prohibiera en 1998 la transmisión de datos personales desde la Unión europea a USA, a la espera de negociar un acuerdo. A su vez, USA acusa a la Unión europea de erigir obstáculos a los intercambios comerciales.

Inmersos en el debate sobre la regulación en Internet, con dos tendencias para lo que se refiere a los comunicados y la difusión de información a través de la red. Una que parte

¹⁰ E. Morón Lerma, *Internet y Derecho pena: Hacking y otras conductas ilícitas en la red*, Pamplona, 2002.

de la libertad de expresión y niega la necesidad de regulación, y otra que la considera imprescindible¹¹.

Siguiendo la mayoría de los países la tendencia de la regulación, en nuestro país, esta se produce conjugando las distintas Directivas europeas con la autorregulación.

Es necesario precisar cuando se habla de Internet, en lo que se refiere a la regulación, para diferenciar; la red global de comunicación, que desde su implantación y desarrollo como red ideal y abierta, no parece exigir otra regulación que la de los nombres de dominio.

Por otro lado, esta la red como medio de comunicación interindividual, pero entre multitud de personas para la recepción y emisión de mensajes, como plataforma de transacciones comerciales y por tanto, bajo el ámbito de aplicación de la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico.

Estamos hablando de los Servicios de la Sociedad de la Información concretados a efectos de la Ley en las obligaciones y responsabilidades de los prestadores de servicios, establecidos en España o de cualquier país del espacio económico europeo.

4.2. LA LEY 34/2002 DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y COMERCIO ELECTRÓNICO

El objeto de esta Ley responde a la necesidad de asegurar una certeza, confianza y seguridad a la hora de contratar bienes y servicios a través de Internet.

La LSSI pretende eliminar uno de los principales obstáculos detectados por los expertos para el despegue del comercio electrónico y del uso de otros servicios de la Sociedad de la Información, la falta de confianza de los usuarios en la seguridad de las transacciones efectuadas por medios electrónicos.

No se puede hablar de la Ley de Internet, porque este no es el único derecho aplicable a las actividades realizadas por vía electrónica, sino que se suma a las normas generales o sectoriales aplicables a la red.

Mediante esta Ley se incorpora al Ordenamiento jurídico español la Directiva 2000/31 del Parlamento y el Consejo europeo.

El objetivo de la Directiva y por tanto, de la ley, es garantizar la libre circulación de los servicios de la sociedad de la información, así como implantar un marco jurídico claro y uniforme que facilite el desarrollo del comercio electrónico en el mercado interior europeo.

La LSSI establece un marco jurídico que pretende garantizar todo tipo de transacciones electrónicas y actividades realizadas a través de los nuevos medios digitales interactivos: Internet, telefonía móvil y televisión digital. Con esta norma se pretende eliminar uno de los principales obstáculos detectados por los expertos para el despegue del comercio electrónico, como es la falta de confianza de los usuarios en la seguridad e las transacciones efectuadas por medios electrónicos.

¹¹ José M. Souviron Morenilla, *Convergencia de los medios de comunicación y regulación de Internet en la Ley de Servicios de la Sociedad de la Información*, Madrid, 2002.

Esta Ley se aplica a todas las actividades que se realicen por medios electrónicos y redes interactivas, tanto a través de ordenador personal como mediante teléfono móvil, el cable o la televisión digital. Y que tengan carácter comercial o persigan un fin económico.

Para garantizar los requisitos de información y transparencia en las comunicaciones la LSSI hace posible que los usuarios tengan elementos de referencia e identificación suficientes de la empresa con la que esta contratando o de la que recibe información, reforzando su seguridad. Con el fin de mejorar la confianza de los consumidores, se establece que los prestadores de servicios de la sociedad de la información deberán comunicar al menos, uno de los nombres de dominio o direcciones de Internet que utilicen habitualmente al Registro Mercantil.

En cuanto a la publicidad no deseada, la LSSI protege a los usuarios al prohibir el envío de publicidad a través del correo electrónico o el teléfono móvil sin el consentimiento previo del destinatario.

La retirada de los contenidos en los medios publicados en Internet sólo puede hacerse por la autoridad judicial. Los prestadores de servicios no están obligados a supervisar o controlar los contenidos que transmiten, siempre que no sean elaborados por ellos. Sus obligaciones se limitan a retirar dichos contenidos o hacerlos inaccesibles, cuando tengan conocimiento efectivo sobre su ilegalidad.

La LSSI garantiza la plena validez de los contratos celebrados por vía electrónica equiparándolos a los escritos y reforzando la eficacia de los documentos electrónicos como prueba ante los Tribunales, con el mismo valor probatorio que los documentos en soporte papel.

Se fomenta al adopción de criterios de clasificación y etiquetado de contenidos para proteger a los niños frente a contenidos indeseables, así como creando subdominios dedicados a actividades educativas y de entretenimiento para menores.

El acceso de los discapacitados a los servicios de la sociedad de la información se contempla en la LSSI, obligando a las Administraciones Públicas a adaptar sus páginas de Internet para el acceso de personas con minusvalía antes del 31 de diciembre del 2005. Así como, promoviendo la fabricación de equipos y programas informáticos adecuados a las necesidades.

La Ley también contempla la participación activa e las asociaciones representativas de los colectivos con discapacidad en la elaboración de los códigos de conducta.

La autorregulación del sector esta prevista mediante los códigos de conducta que se elaboran con la participación de las asociaciones empresariales, profesionales y de usuarios afectados. Se promueve así mismo, el establecimiento de sistemas de resolución extrajudicial de conflictos homologables con los principios comunitarios y con la garantía del Consejo de Consumidores y Usuarios.

Esta regulado también la “acción de cesación” que se ejercita ante los Tribunales de la Civil para obtener de forma rápida el cese de las conductas que lesionan los intereses colectivos de consumidores y usuarios, incluso de aquellas originadas en otros Estados miembros de la Unión Europea.

5. CONCLUSIONES

Nos hemos acercado al análisis de la tecnología informática, 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. Por ello se ha hecho imprescindible la necesidad de regulación, en nuestro país a través de la Ley de Servicios de la Sociedad de la Información y el Comercio electrónico.

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.

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. Esto se ve reforzado por la Sentencia 292/2000 que reconoce la categoría de derecho fundamental a la protección de datos personales.

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.

RESUMEN: La Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico ha permitido la regulación de aspectos que inciden en la protección de Derechos Fundamentales como son la intimidad y el propio honor en el uso de las nuevas tecnologías de la información y la comunicación a través de la protección de los datos personales en Internet.

ABSTRACT: The “Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico” has permitted the regulation of aspects that affects fundamentals rights safeguard as privacy and personal honour in the information and communication new technologies with the private data safeguard in Internet.

