

LA PROTECCIÓN DE DATOS Y LAS COMUNICACIONES ELECTRÓNICAS

Miguel Ángel DAVARA RODRÍGUEZ

SUMARIO: I. *Introducción*. II. *Una primera aproximación a la protección de datos*. III. *La conciencia europea sobre protección de datos*. IV. *El derecho fundamental: la sentencia 292/2000 del Tribunal Constitucional Español*. V. *La Directiva Europea sobre Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas*. VI. *A modo de conclusión*.

I. INTRODUCCIÓN

Me parece arriesgado abordar el tema de la protección de datos en el ámbito de las comunicaciones electrónicas aun en el caso de que lo hiciera en el marco de la difusión desenfadada, incluso casi irresponsable, en la que, en ocasiones, nos vemos obligados a movernos los que estamos a menudo pendientes de la imprenta.

Además, siempre que me pongo a escribir sobre cualquier cuestión relativa a protección de datos, siento un desequilibrio emocional difícil de contener. Por un lado me pregunto, y rechazo al mismo tiempo, sobre la mayor o menor bondad de la normativa que, en ocasiones hasta distante, va viendo la luz en determinados lugares; por otra parte, siento que estas

* Ingeniero y doctor en derecho; catedrático de Derecho informático y de informática para juristas de la Facultad de Derecho de la Universidad Pontificia Comillas de Madrid (ICAI-ICADE); director de la *Revista Actualidad Informática* de Aranzadi; miembro del Grupo de Asesores Legales en Tecnologías de la Información de la Unión Europea en Luxemburgo (DG Sociedad de la Información), y autor de libros y artículos sobre derecho e informática.

normas son muy teóricas y poco realistas cuando se mueven en terrenos escabrosos en el ámbito de la práctica diaria.

Pero, en este caso, todas estas cuestiones se agrandan, y mi responsabilidad se hace mayor, al tener la osadía de escribir en una obra que recibe tan magníficos trabajos, de tan insignes autores y en homenaje a tan ilustre jurista, como es el doctor Héctor Fix-Zamudio, con motivo de sus cincuenta años como investigador jurídico.

No obstante, con la irresponsabilidad propia del adicto a la pluma, me pongo a trabajar sobre la cuestión y vienen a mi mente dos documentos que considero básicos: uno de ellos, de carácter casi romántico, incluso podemos decir que con algunos detalles de musa, es la resolución (73) 22, del Consejo de Europa, relativa a la “protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado”,¹ y el otro, con todo el sabor de fuente de sabiduría, riguroso, casi podríamos decir que netamente científico, es el denominado Convenio 108 del Consejo de Europa.²

Ambos documentos traen melancólicamente a mi presencia, veo y toco los folios ya amarillentos en los que conservo la primera copia que manejé, la, en mi opinión magnífica, pero ya derogada, Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD).³ Cuántos gratos recuerdos de aquellos primeros pasos en los que posiblemente llegué a saber algo sobre protección de datos con la ilusión propia de los comienzos, la osadía de la ignorancia y la rapidez por absorber todo lo que veía y tocaba sobre la materia, prisa incontenible que

¹ Adoptada durante la 224 reunión de los Delegados de los Ministros, el 26 de septiembre de 1973.

² Convenio número 108, del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este Convenio fue firmado en Estrasburgo por el plenipotenciario de España el 28 de enero de 1982, ratificado mediante instrumento del 27 de enero de 1984, y publicado en el *Boletín Oficial del Estado* núm. 274, del 15 de noviembre de 1985. El Convenio entró en vigor el 1o. de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo. En adelante lo citaremos como el Convenio 108.

³ Ley Orgánica 5/1992, del 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, publicada en el *Boletín Oficial del Estado* núm. 262, del 31 de octubre. La LORTAD fue la primera ley española sobre protección de datos que, de alguna forma, educó en la materia a múltiples titulares de ficheros, tanto de titularidad pública como privada.

exigía el saber que tenía mucho tiempo por delante pero muchas más cosas por hacer.

Varios años más tarde, décadas en el caso de la Recomendación del Consejo de Europa, me siento ante el ordenador con temor y preguntándome de nuevo si tendré algo que decir o si caeré en la valentía inconsciente de opinar desde la tribuna generosa que me proporciona quien publica este trabajo; pero, respondiendo a esa generosidad, seré, por lo menos, serio y dedicaré mi tiempo y esfuerzo a responder, si quiera en parte, a esta confianza.

De esta forma diré que me aproximo a este trabajo con vocación de análisis o solamente de estudio interpretativo de una cuestión que, cada día más, alcanza al desorden conceptual que todos vamos teniendo alrededor de la protección de datos.

Parecía que ya habíamos llegado al punto de tener o conocer una seria doctrina en el alcance de esta normativa, y que el tiempo pasado desde aquellos primeros estudios en el seno del Consejo de Europa⁴ había proporcionado la base sobre la que nos encontráramos sólidos y amparados para poder opinar partiendo de unas premisas por todos aceptadas.

Pero esto no es así; no sé si es el afán por saber y conocer, o simplemente las distintas y, en ocasiones, distantes opiniones vertidas desde los lugares que deberían equilibrar los razonamientos jurídicos, pero lo cierto es que la inseguridad en el momento de ahondar sobre determinadas cuestiones se presenta a cada instante como fantasma que impide nuestros movimientos intelectuales, y que nos sitúa en un lugar de aceptación de teorías y de opiniones, para utilizarlas y aplicarlas en el devenir profesional diario en la obligación, que todos los docentes tenemos, de transmitir conocimientos y experiencias, para que nuestros alumnos tengan un punto de partida y de referencia sólido que les permita desarrollar sus capacidades de entendimiento y aprendizaje.

4 Desde el lejano 1967 que, en el seno del Consejo de Europa, se constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad a los más elementales derechos de la persona, trabajo que dio como fruto la Resolución 509, de 1968, de la Asamblea del Consejo de Europa, sobre “los derechos humanos y los nuevos logros científicos y técnicos”, hasta la caótica situación actual en la realidad normativa sobre protección de datos de los países de nuestro entorno socio cultural, han pasado muchos años de estudios, trabajos, investigaciones, desarrollos normativos, interpretaciones administrativas y de otros órganos con diferentes estructuras y jerarquías.

Me refiero, en particular, al tema que abordo en este trabajo que, siendo de gran interés en la práctica diaria, tantas dificultades de interpretación me trae cuando ahondo en cuestiones específicas. Se trata de la protección de datos y las comunicaciones electrónicas.⁵

Pero antes quisiera, casi como recordatorio para mí con el fin de poder seguir el hilo de exposición que pretendo, abordar una primera aproximación a la protección de datos.

II. UNA PRIMERA APROXIMACIÓN A LA PROTECCIÓN DE DATOS

Si entendemos por dato el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad, y aceptamos que ese dato se encuentra en un documento o soporte —físico o lógico— con la calidad de testimonio, debemos diferenciarlo de información, entendiendo por tal la acción de informar o dar noticia de algo. Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuesta o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución a un problema, se ha convertido en información.

Comenzaremos diferenciando la documentación como conjunto de datos, noticias o pruebas que se refieren a un determinado asunto, y la información entendida como esa misma documentación estructurada en función de determinados fines.

El dato, por tanto, o la documentación —entendida como conjunto de datos— son las noticias en su origen, sin haber sido sometidas a ningún tipo de tratamiento ni adecuación. Cuando el dato o la documentación —como conjunto de datos— es sometida a un tratamiento o adecuación a un fin, para obtener un resultado elaborado, se convierte en información, y ésta será el resultado orientado y adecuado a un fin determinado.

⁵ Creemos necesario en este apartado introductorio destacar que este trabajo contempla la situación de la protección de datos y las comunicaciones electrónicas en el ámbito territorial de la Europa Comunitaria y, en particular, de España; es de esta forma como está escrito y, naturalmente, como rogamos sea entendido.

La información contribuye de una forma directa a la difusión de conocimientos y, consecuentemente, a la formación de las personas. Su explosión y alcance se multiplica al intervenir los medios de comunicación que, con su gran capacidad de difusión de información y acercamiento en tiempo y en espacio, hacen pensar en unos grandes e influyentes agentes de cambio que proporcionen mayor riqueza a la información, con su consiguiente optimización de conocimientos, mejorados por su utilización y adaptación al entorno al ser utilizados.

La informática, entendida como la ciencia del tratamiento automático de la información, con las posibilidades que ofrece de almacenamiento y tratamiento de la documentación y la recuperación de la información registrada en soportes magnéticos, ópticos u otros, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control social.

Por otra parte, la complejidad de la sociedad actual obliga a proporcionar, más o menos voluntariamente, determinados datos personales a instituciones, públicas o privadas, que siempre bajo la aureola del bien común, del interés social, o para facilitar un servicio determinado con mayores garantías de eficacia, los introducen en ordenadores, donde pueden ser procesados y utilizados de forma que escapen a nuestro control.

El ordenador, con su gran velocidad de cálculo, puede comparar, contrastar los datos acerca de un individuo, introducidos en su memoria, y señalar aquéllos que se desvíen de un *standard* previamente establecido. Realizará, o podrá realizar, una función de control, comparando la imagen real de los datos del individuo en cuestión, con otra imagen —llamémosla “ideal”— que se había seleccionado, buscando dónde existe desviación y proporcionando información sobre esa desviación.

La ayuda que, por otro lado, proporcionan las comunicaciones, y, en particular, las comunicaciones electrónicas y la transferencia de datos telemática entre ordenadores permite el cruce de ficheros y registros informáticos, con su correspondiente proceso y tratamiento automático de la información mediante los programas adecuados.

Es así como llegamos, en un principio, a la llamada protección de datos o a la protección que las normas contemplan para el titular de los datos. Es la persona titular de los datos la que puede necesitar la protección, ya que el dato, como tal, no necesita protección alguna.

La protección del titular de los datos

En primer lugar destacaremos que se trata de proteger a las personas ante el manejo o manipulación, no autorizada, de sus datos personales, con especial atención cuando estos datos sean susceptibles de tratamiento automatizado o se encuentren en un soporte susceptible de tratamiento automatizado.

Si los datos se encontraran en un soporte no susceptible de tratamiento automatizado, ya que la organización y estructura del fichero manual no permitiera el acceso con arreglo a criterios determinados, o no fuera posible, por la razón que sea, su tratamiento informático, no tendría tanto sentido y alcance esta protección. Es en el carácter y la calidad de informatización —o posible informatización—, y en las características y consecuencias del tratamiento informático de los datos donde adquiere mayor fuerza esta necesidad de protección.

En segundo lugar, el resultado de la elaboración de los datos debe ser identificable con el titular de los mismos, o que se pueda identificar a esta persona a través de este resultado, llegando, incluso, a conocer nuevas características de su personalidad y de su entorno o esfera íntima, como consecuencia del mismo.

En tercer lugar, tiene que darse un manejo de los datos —o un acceso a los datos— sin consentimiento de su titular, o para fines diferentes a los que el titular autorizó o se vio obligado a dar los datos.

En resumen, tres son las características básicas con las que delimitamos el estudio de la llamada protección de datos:

- a) Que los datos sean susceptibles de tratamiento o se encuentren en soporte susceptible de tratamiento.
- b) Posibilidad de identificar el resultado del tratamiento de los datos —la información como dato elaborado hacia un fin— con el titular.
- c) El manejo o acceso a los datos sin consentimiento —o con conocimiento, según los casos— del titular, independientemente de que este acceso o manejo sea en forma malintencionada o no. La persona titular de los datos puede perder totalmente el control sobre la utilización de los mismos y el tratamiento al que se les puede someter.

Todos estos datos, organizados y estructurados deben estar protegidos contra el acceso —malintencionado o no— de quienes no estén autorizados para ello. La protección se realiza, consiguientemente, sobre el dato, para que éste no pueda ser tratado o elaborado, y convertido en información, nada más que para aquellos fines y por aquellas personas autorizadas a ello.

Esta necesaria protección es un límite, en su caso, a la utilización de la informática ante el temor de que pueda agredir a la intimidad de los ciudadanos, personal o familiarmente, y que pueda coartar el ejercicio de sus derechos.

De esta forma, tenemos la llamada protección de datos, entendida como la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal, o, expresado de otra forma, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad, y que es un tema que ha adquirido enorme actualidad, casi diríamos protagonismo, y que afecta directamente a un derecho fundamental de elevado contenido.

III. LA CONCIENCIA EUROPEA SOBRE PROTECCIÓN DE DATOS

Como ya hemos indicado, desde aquel lejano 1967, por fijar una fecha de comienzo, en el que, en el seno del Consejo de Europa, se constituyó una comisión consultiva para estudiar las tecnologías de la información y su potencial agresividad a los más elementales derechos de la persona, que concluyó con la resolución 509 de 1968, de la Asamblea del Consejo de Europa, sobre “los derechos humanos y los nuevos logros científicos y técnicos”, hasta las directivas europeas 95/46/CE, 2002/58/CE, que tratamos en este trabajo, y 2006/24/CE⁶, pasando por las didácticas resoluciones (73) 22 y (74) 29 del Comité de Ministros del Consejo de Europa

⁶ Directiva sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE (*DOL* 105 del 12 de abril).

sobre la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos tanto en el sector privado como en el público y, naturalmente, por el Convenio (108) del Consejo de Europa, relativo a la “protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”, del 28 de enero de 1981, la conciencia europea ha sido rica y fecunda, y relativamente sensible, al proteger al ciudadano ante esta potencial agresividad de la informática a la intimidad de la persona.

Varias son las normas que, teniendo por objeto la “protección de datos”, han visto la luz en los últimos años en lo que podíamos llamar la “conciencia europea sobre protección de datos”, y todas ellas están ayudando a formar una cultura básica sobre el denominado principio de la autodeterminación informativa centrado en el concepto de que los datos no son propiedad de quien los posee o maneja, sino que los datos son propiedad de su titular, del ciudadano, y solamente él tiene derecho a decidir quién, dónde, cuándo y cómo los presenta al exterior, en el que ha adoptado ya carta de naturaleza, principio de la autodeterminación informativa.

En el ámbito europeo el camino ha sido firme y decidido en la protección del ciudadano ante esa potencial agresividad de la utilización de las tecnologías de la información y las comunicaciones (TIC) a aspectos incluso más profundos que su propia intimidad.

1. *El Convenio 108 del Consejo de Europa*

De entre las normas citadas cabría destacar el conocido Convenio 108⁷ que es sin duda uno de los documentos de mayor importancia de todos los que han visto la luz sobre este tema en el seno del Consejo de Europa.

El Convenio tiene por objeto (artículo 1o.) garantizar en el territorio de cada parte, a cualquier persona física, el derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal.

Se podría pensar —de acuerdo con lo establecido en la Constitución Española (artículo 96.1), que al referirse a los tratados internacionales

⁷ Convenio (108) para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, del 28 de enero de 1981, firmado en Estrasburgo por el plenipotenciario de España el 28 de enero de 1982, ratificado mediante instrumento del 27 de enero de 1984, y publicado en el *Boletín Oficial del Estado*, núm. 274, del 15 de noviembre de 1985.

válidamente celebrados, expresa que “una vez publicados oficialmente en España, formarán parte del ordenamiento interno”— que el Convenio forma parte de nuestro ordenamiento interno y, por tanto, es, a partir de su publicación, la “norma española” sobre protección de datos. Efectivamente, el Convenio es, desde entonces, la norma española de protección de datos, pero hay que tener en cuenta que no es una norma de aplicación directa o de efecto directo, ya que (artículo 4.1) remite a los propios Estados firmantes para que desarrollen leyes y adopten medidas, a fin de que se pueda dar cumplimiento a los principios enunciados en su texto.

Pero, independientemente de que el Convenio sea o no de aplicación directa, lo cierto es que el cumplimiento de su contenido normativo ha sido compromiso adquirido por España.

Entrando en el contenido del Convenio queremos resaltar algunos aspectos que expondremos en tres apartados que resumen y reflejan las partes fundamentales y los conceptos que recoge. Éstos son:

- a) Consideraciones generales.
- b) Principios y garantías.
- c) Sanciones y procedimiento.

A. Consideraciones generales

En primer lugar haremos referencia a algunas definiciones contenidas en el texto del Convenio, que tienen por finalidad centrar los conceptos sobre los que gira la norma marco. De esta forma se entiende por (artículo 2o.):

- Datos de carácter personal, cualquier información relativa a una persona física identificada o identificable.
- Fichero automatizado, cualquier conjunto de información que sea objeto de un tratamiento automatizado.
- Tratamiento automatizado, las operaciones de registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión, efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados.
- Autoridad controladora del fichero, la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea com-

petente para decidir cuál será la finalidad del fichero automatizado, qué categorías de datos de carácter personal deban registrarse y qué operaciones se les aplicarán.

En segundo lugar resaltaremos que el Convenio no distingue entre ficheros de titularidad pública y ficheros de titularidad privada, indicando (artículo 3o.) que se aplica tanto a los sectores público como privado, y (artículo 4o.) que cada parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos, dejando a cada parte (artículo 11) la posibilidad de conceder a los afectados una protección más extensa que la prevista en el Convenio.

B. Principios básicos para la protección de datos

Dentro de los denominados principios básicos para la protección de datos, el Convenio distingue cinco apartados:

1. La calidad de los datos, comprendiendo la exigencia de que los datos se deben obtener y tratar leal y legalmente, deben ser registrados para finalidades determinadas y legítimas, serán adecuados, pertinentes y no excesivos en relación con las finalidades para las que se recabaron y registraron, y serán exactos y puestos al día.
2. Categorías particulares de datos que no podrán tratarse automatizadamente, a menos que el derecho interno prevea las garantías apropiadas. Estas categorías particulares de datos recogen los datos relativos al origen racial, opiniones políticas, convicciones religiosas u otras creencias, la salud, la vida sexual y las condenas penales.
3. Seguridad de los datos, con la exigencia de que se deben adoptar en el tratamiento automatizado de datos las medidas de seguridad necesarias para evitar la destrucción accidental, la pérdida accidental y el acceso, la modificación o la difusión no autorizada a los datos.
4. Garantías complementarias para la persona, centradas en los denominados derechos de información, acceso, rectificación y borrado, así como de disposición de un recurso; estos derechos deben garantizar que la persona pueda: a) conocer la existencia del fichero, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fi-

chero; *b*) obtener en intervalos razonables, y sin demora o gastos excesivos, la confirmación de la existencia o no en el fichero automatizado de los datos de carácter personal que le conciernan, así como la comunicación de dichos datos en forma inteligible, y *c*) obtener, en su caso, la rectificación o el borrado de los datos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos de calidad de los datos.

5. Excepciones y restricciones, de forma que se puedan establecer excepciones cuando, previstas en una ley, constituyan una medida necesaria para la protección de la seguridad del Estado, de la seguridad pública, los intereses monetarios del Estado o la represión de infracciones penales, así como para la protección de la persona y los derechos y libertades de otras personas. También contempla que mediante ley se podrán prever restricciones en el ejercicio de los derechos de la persona concernida cuando se trate de ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, siempre que no existan riesgos manifiestos de atentado a la vida privada de las personas concernidas.

C. Sanciones y procedimiento

Se prevé en el Convenio (artículo 10) la posibilidad de establecer sanciones y recursos, indicando que cada parte se compromete a establecer las correspondientes sanciones contra las posibles infracciones, así como que establecerá un procedimiento de cooperación entre ellas para prestarse asistencia para el cumplimiento del Convenio, a cuyo fin (artículo 13) se designará una o más autoridades, cuya denominación y dirección se comunicará al secretario general del Consejo de Europa.

IV. EL DERECHO FUNDAMENTAL: LA SENTENCIA 292/2000 DEL TRIBUNAL CONSTITUCIONAL ESPAÑOL

En el ámbito territorial español podemos decir que encontramos dos momentos claramente diferenciados en lo que respecta a la interpretación de la normativa sobre protección de datos; podemos decir que hay un an-

tes y un después, marcados el 30 de noviembre de 2000, fecha de la de publicación de la sentencia 292/2000 del Tribunal Constitucional.

Esta sentencia es consecuencia del recurso de inconstitucionalidad interpuesto por el defensor del pueblo contra los artículos 21.1 y 24.1 y 2o. de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD),⁸ publicada en el *Boletín Oficial del Estado* núm. 298, del 14 de diciembre; al considerar (el defensor del pueblo) que la comunicación de datos entre las administraciones públicas en la forma en que, excepcionalmente, quedaba permitida por lo dispuesto en el apartado 1, del artículo 21 de la LOPD, así como las excepciones a los derechos de los afectados previstas en los apartados 1 y 2 del artículo 24, del mismo cuerpo legal, lesionaban, ambas cuestiones, el contenido esencial de los derechos fundamentales del artículo 18.1, en relación con lo dispuesto en el artículo 18.4, de la Constitución Española, así como la reserva de ley propugnada en el artículo 53.1 de la norma constitucional.

La referida sentencia, estimando el recurso de inconstitucionalidad interpuesto, que era el fondo del asunto, resulta rica en interpretaciones que, figurando en sus fundamentos jurídicos y entrando en cuestiones que afectan al contenido conceptual de las teorías sobre protección de datos, condicionan en gran medida la línea doctrinal, e incluso, simplemente argumental, que por diversos autores se hacía en esta materia.

Hasta entonces había incluso opiniones tendentes a negar, o no aceptar como tal, el denominado derecho fundamental a la protección de datos. De una manera sencilla y rotunda, con nitidez en la exposición, deja claro la propia sentencia⁹ que el “derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad... atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos...”, continuando con el reforzamiento de las potestades del individuo al resaltar que ese derecho fundamental a la protección de datos¹⁰ “garantiza a los individuos un poder de disposición sobre esos datos... que... nada vale si el afectado desconoce qué datos son los que poseen terceros, quiénes los poseen y con qué fin”.

⁸ Ley de Protección de Datos actualmente vigente en España.

⁹ En el último párrafo del Fundamento Jurídico 5.

¹⁰ Primer párrafo del Fundamento Jurídico 6.

Quedando claro de esta forma, y también porque lo indica la propia sentencia,¹¹ que el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, “sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 de la CE otorga, sino los datos de carácter personal”.

Muchas otras cosas se podrían decir analizando esta sentencia pero, a los efectos que perseguimos en este trabajo, es suficiente con lo indicado, recalcando que:

- a) Se trata de un derecho fundamental —el derecho fundamental a la protección de datos—.
- b) Que es independiente y autónomo del derecho a la intimidad.
- c) Que no se reduce a los datos íntimos de la persona sino a cualquier tipo de dato personal sea o no íntimo, garantizando al titular de los datos un poder de disposición sobre los mismos asociado al poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos.

En el ámbito de las comunicaciones electrónicas y la necesidad de tratamiento de estos datos de carácter personal por los operadores de telecomunicaciones y por los prestadores de servicios de intermediación en redes, destaca este poder de disposición sobre los datos de su titular que puede afectar al comportamiento de las empresas en sus relaciones comerciales otorgando un protagonismo legítimo al ciudadano, que será el que podrá decidir en cada caso, con las excepciones legales que se contemplan, cuándo, dónde, cómo y por quién se tratan sus datos.

V. LA DIRECTIVA EUROPEA SOBRE PROTECCIÓN DE LA INTIMIDAD EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS

Entrando ya, y de lleno, en el ámbito de las comunicaciones electrónicas, en este trabajo vamos a centrarnos, en particular y con mayor énfasis,

¹¹ Tercer párrafo del Fundamento Jurídico 6.

sis, en lo especificado en la Directiva 2002/58/CE, sobre la protección de la intimidad en el sector de las comunicaciones electrónicas.¹² Esta Directiva tiene por objeto la denominada protección de datos en el referido sector complementando a la Directiva 95/46/CE,¹³ que podemos considerar como la norma básica de obligado cumplimiento en el ámbito general de protección de datos referido al territorio comunitario europeo.

Uno de los aspectos que se debe destacar al presentar esta Directiva es que nace impulsada por la necesidad de adaptar las normas existentes al desarrollo tecnológico. Las normas deben tener una orientación neutral desde la óptica tecnológica y, aunque no pueden, ni deben, ser ajenas al mercado y al desarrollo, no pueden tampoco depender de ellos más que en la medida en que la implicación social lo demande. La solvencia de las normas que se centren en la denominada sociedad de la información se verá más enriquecida en cuanto logren mantener actitudes de independencia del mercado y del desarrollo tecnológico.

También es necesario tomar en consideración, para mejor exponer los enunciados de esta Directiva, el fenómeno que rodea a Internet, en el que concurren sujetos específicos, tales como el operador de telecomunicaciones, el proveedor de acceso a Internet, el proveedor de servicios de Internet e, incluso, los proveedores de servicios de intermediación y los que simplemente denominan las normas proveedores de servicios de información, que para el desarrollo de su actividad y la prestación de sus servicios requieren del tratamiento de los datos de los usuarios, y que, por tanto, quedan sometidos a la normativa sobre protección de datos general y específica en el sector de las telecomunicaciones y, más en particular, en el sector de las comunicaciones electrónicas.

¹² Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, del 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, publicada en el *Diario Oficial de las Comunidades Europeas* serie L 201, del 31 de julio de 2002. En adelante y para facilitar la lectura, nos referiremos a ella también como la Directiva sobre la Privacidad y las Comunicaciones Electrónicas.

¹³ Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre, 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, publicada en el *Diario Oficial de las Comunidades Europeas*, núm. L 281, del 23 de noviembre de 1995, pp. 31-50, en adelante, también, la Directiva General de Protección de Datos o la Directiva 95/46/CE.

1. *El concepto de comunicaciones electrónicas*

Si se habla de servicios de comunicaciones electrónicas y redes de comunicaciones electrónicas, en lugar de servicios de telecomunicaciones y redes de telecomunicaciones, es consecuencia del fenómeno de convergencia que ha sido auspiciado, al modo de señales prósperas que en el comienzo de la actividad parecen presagiar el resultado, por la unión de diferentes coordenadas consecuentes del desarrollo tecnológico.

Estas definiciones nuevas son indispensables para tener en cuenta el citado fenómeno de convergencia, agrupando en una sola definición todos los servicios y redes de comunicaciones electrónicas relacionados con el transporte de señales, y su decidida consecuencia es la apertura a una más amplia comprensión, al tiempo que conocimiento y difusión, de nuevos servicios y más amplias aplicaciones, con lo que todo ello tiene de positivo pero con lo que puede tener de potencial agresividad a los más elementales derechos de la persona.

El aspecto más relevante que consideramos necesario señalar en este momento de introducción al concepto es que la Directiva Europea sobre la Privacidad y las Comunicaciones Electrónicas hace referencia a los *servicios de comunicaciones electrónicas y redes de comunicaciones electrónicas*, en lugar de a *servicios de telecomunicaciones y redes de telecomunicaciones*.

Se trata de un concepto más amplio, que en absoluto desplaza a los anteriores, sino que permite obtener un campo de actuación y de interpretación que engloba una realidad social imperante y un mayor ajuste a las nuevas posibilidades que se abren como consecuencia del desarrollo tecnológico.

Buscando una definición que aproxime este nuevo campo de acción, o esta mayor amplitud de conceptos, debemos acudir al considerando (7) de la Directiva Europea 2002/77/CE, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas,¹⁴ que indica que:

¹⁴ Directiva 2002/77/CE, de la Comisión, del 16 de septiembre, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas, publicada en el *Diario Oficial de las Comunidades Europeas*, L 249, del 17 de septiembre.

se habla de “servicios de comunicaciones electrónicas” y “redes de comunicaciones electrónicas”, en vez de “servicios de telecomunicaciones” y “redes de telecomunicaciones”... Estas definiciones nuevas son indispensables para tener en cuenta el citado fenómeno de convergencia, agrupando en una sola definición todos los servicios y redes de comunicaciones electrónicas relacionados con el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos (esto es: redes fijas, inalámbricas, de televisión por cable y por satélite). Así pues, la transmisión y radiodifusión de programas de radio y de televisión deben considerarse un servicio de comunicación electrónica, de la misma manera que las redes utilizadas para tal transmisión y radiodifusión deben considerarse comunicaciones electrónicas. Asimismo, debe quedar claro que la nueva definición de redes de comunicaciones electrónicas también incluye las redes de fibra que permiten a terceros transmitir señales con sus propios equipos de transmisión o conducción.

Como bien indica el citado considerando, las definiciones nuevas y de mayor amplitud de servicios de comunicaciones electrónicas y redes de comunicaciones electrónicas, que agrupan y relacionan todos los conceptos de forma que queda establecido un marco común y uniforme de actuación, son indispensables para tener en cuenta el fenómeno de convergencia que ha caracterizado en los últimos tiempos a los sectores de las tecnologías de la información, los medios de comunicación y las telecomunicaciones.

Es de esta forma que se justifica el nuevo texto, que ha sido provocado por el desarrollo tecnológico y la necesidad de agrupar conceptos y asociar contenidos en una figura más amplia y real al fenómeno que se está viviendo, y que gira en la convergencia de los referidos sectores de las tecnologías de la información, los medios de comunicación y las telecomunicaciones.¹⁵

¹⁵ La propia Directiva 2002/77/CE define en su artículo 1o., qué se entiende por “red de comunicaciones electrónicas”, indicando que comprende “los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la difusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada” y, también en su artículo 1o., define qué

2. *La propia directiva*

La mencionada Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas vino a sustituir a la 97/66/CE, del 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones,¹⁶ que estaba pidiendo a gritos su adaptación al profundo cambio que están experimentando los mercados y la oferta de servicios a través de Internet, ya que con la utilización de la red se introducen nuevas posibilidades para los usuarios, pero también se producen nuevos riesgos para sus datos personales y su intimidad.

El objeto de esta Directiva sobre la Privacidad y las Comunicaciones Electrónicas se centra, como ya hemos indicado, en la armonización de las disposiciones de los Estados miembros para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la comunidad.

Es, en definitiva, un paso más para garantizar la seguridad jurídica y los derechos fundamentales de las personas con la utilización, no sólo de las redes de telecomunicaciones, sino en el más amplio campo, y sin duda, más complejo, de las comunicaciones electrónicas.¹⁷

se entiende por “servicios de comunicaciones electrónicas”, indicando que es “el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos”. Creemos que estas definiciones permiten clarificar por sí solas los conceptos que venimos utilizando.

¹⁶ Publicada en el *Diario Oficial de las Comunidades Europeas (DOCE)*, del 30 de enero de 1998, pp. L24/1-L24/8, que, según expresa en su preámbulo, tiene por objeto, además de ultimar la incorporación de normativas comunitarias, la determinación de los derechos de los usuarios finales en la prestación de los servicios que se consideran de carácter público y la regulación de los aspectos técnicos de la protección de los datos personales en las redes de telecomunicaciones.

¹⁷ También habría que considerarla como un nuevo impulso normativo al comercio electrónico, potenciando su utilización al tiempo que garantizando el respeto a unos dere-

¿Se ha producido realmente ese giro radical que exige nuevas mentalidades en la cultura básica de protección de datos?; pensamos que no, pero es necesario que hagamos un esfuerzo interpretativo para poder decir esto con seguridad; es por ello que no entramos, todavía, a profundizar sobre su alcance, y esperamos tiempos, precedidos de mayores posibilidades de estudio, para poder asegurar si estamos en lo cierto sobre su significado o se trata nada más que de un objeto retórico.

Entre las cuestiones más significativas a destacar sobre protección de datos en las comunicaciones electrónicas que recoge la propia Directiva, señalamos el “tratamiento por terceros de datos sobre tráfico y facturación” sobre el que la Directiva indica que sólo podrán encargarse del tratamiento de datos de tráfico las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.

Merece especial atención también lo referente a datos que figuran en guías de servicios de telecomunicaciones disponibles al público sobre los que la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, poniendo el dedo en la llaga de los problemas que se suscitan, comienzan por exponer el potencial peligro a la intimidad de la persona que contienen estos directorios, necesarios pero, a veces descontrolados, en su difusión y utilización.¹⁸ La posibilidad de su acceso telemático, con la utilización de potentes herramientas, pueden convertirlos en una fuente inagotable de problemas si no se delimita claramente cómo pueden ser utilizados.

Al considerarles como fuentes accesibles al público y al quedar éstas prácticamente exceptuadas del principio del consentimiento tanto en el

chos básicos irrenunciables que no pueden ceder ante el imparable aumento de la contratación electrónica, pero no es este el lugar para profundizar en el tema.

¹⁸ “Las guías de abonados a los servicios de comunicaciones electrónicas alcanzan gran difusión y tienen carácter público”, comienza diciendo con rotundidad el primer párrafo del considerando 38 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas.

tratamiento como en la cesión o comunicación de datos, es exigible una bien definida regulación que permita equilibrar la permisividad aducida con una elemental protección ante tratamientos en cadena.

No se trata solamente de accesos inversos,¹⁹ que ya de por sí no están autorizados, sino de la posibilidad de tratamientos de estos datos con otros datos estadísticos o conocidos sin mayores problemas por figurar también en otras fuentes accesibles al público,²⁰ que permiten el cruce de todos ellos y, mediante adecuados programas de simulación con la aplicación de los pertinentes parámetros, traerían como consecuencia la obtención de otros datos que no solamente no se encuentran en fuente accesible al público alguna si no que, incluso, son desconocidos para su titular.

Es por todo ello que la Directiva sobre la Privacidad y las Comunicaciones Electrónicas presenta una dedicación específica y especial al tratamiento de estos datos, indicando en su considerando 39 que debe existir una obligación de informar en todas las fases, tanto cuando se recaban los datos, como cuando se comunican a terceros, además de informar también sobre los tratamientos a los que serán sometidos, exigiendo nuevamente la obtención del consentimiento cuando un tercero a quien se hayan transmitido los datos quisiera utilizarlos con un fin suplementario.

Especial atención, y elogio, nos merece lo contemplado en el artículo 12 de la Directiva que, bajo el epígrafe de “guías de abonados”, exige, no solamente la información gratuita a los abonados antes de ser incluidos

¹⁹ En este sentido, el último párrafo del considerando 38 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, deja claramente expresado que los suministradores de guías públicas “deben informar a los abonados que vayan a incluirse en tales guías acerca de la finalidad de las mismas y de cualquier uso particular que pueda hacerse de las versiones electrónicas de las guías públicas, especialmente a través de funciones de búsqueda incorporadas al soporte lógico, tales como las funciones de búsqueda inversa que permiten al usuario de la guía averiguar el nombre y la dirección del abonado a partir exclusivamente de un número de teléfono”.

²⁰ Como, por ejemplo, Boletines Oficiales, medios de comunicación o, incluso, listas de personas pertenecientes a grupos de profesionales que contengan los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, en expresión literal del apartado j) —fuentes accesibles al público— del artículo 3o., de la LOPD. Estos datos, adecuadamente tratados con otros datos estadísticos, sociológicos y económicos, obtenidos de informaciones y constantes explicativas de la evolución económica o social de un determinado territorio, permiten obtener un perfil profundo de la persona que ella misma desconoce y, lo que es peor, no puede valorar al faltarle los elementos y parámetros necesarios para ello; sin embargo, son datos suyos, del titular, del que, tristemente, no puede conocer ni valorar su significado y alcance.

en las guías sobre los fines de estas guías, ya sean impresas o electrónicas, sino también sobre cualquier posibilidad de uso que, particularmente y por sus características, se pueda hacer con base en funciones de búsqueda en las versiones electrónicas de la guía.

El principio de la finalidad,²¹ con las características propias de adecuación y pertinencia, se encuentra recogido en el texto de la Directiva como exigencia básica para la inclusión de los datos, con el consentimiento cuando sea preciso y, en todos los casos, sea o no preciso, con el conocimiento por medio de una clara y transparente información.

Debemos resaltar que la finalidad de una guía no la define el proveedor, sino que queda claramente delimitada, en cuanto a los mínimos,²² en la propia Directiva, fijándose en la búsqueda de datos de contacto de personas a partir de su nombre y, “si resulta necesario, de un mínimo de otros identificadores”,²³ siendo necesario el consentimiento específico de los abonados para cualquier finalidad distinta.

En relación con las llamadas no solicitadas con fines de venta directa, teniendo en cuenta que la prospección comercial y la venta directa se presentan como temas conflictivos cuando se trata de analizar y de proteger el derecho a la intimidad, máxime en el caso, cada día más frecuente, de las llamadas telefónicas no solicitadas para venta directa, indica la Directiva que cuando se obtenga de los clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE,²⁴ se podrán utilizar dichas señas

²¹ Este principio de la finalidad, que está recogido en el artículo 4 —calidad de los datos— de nuestra vigente Ley de Protección de Datos, indicando que “los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”, queda también contemplado con nitidez en el apartado 2, del artículo 12 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, al indicar que “Los Estados miembros velarán porque los abonados tengan oportunidad de decidir si sus datos personales figuran en una guía pública, y en su caso cuáles de ellos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor”.

²² Incluso en cuanto a los máximos que no exigirían el consentimiento sino solamente la exclusión voluntaria por el abonado si lo considera oportuno.

²³ En expresión literal del apartado 3, del artículo 12 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas.

²⁴ Directiva a la que nosotros venimos denominando como “general de protección de datos”.

electrónicas para la venta directa de sus productos o servicios de características similares, siempre y cuando se ofrezca a los clientes con claridad²⁵ la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado su utilización, cada vez que reciban un mensaje posterior.

Es como si se tratara de un ofrecimiento constante, en cada comunicación que se haga, para que, si es de su interés, no reciba más comunicaciones comerciales a través del correo electrónico. Parece evidente que se está previendo un sistema de información dinámico que puede ser entendido como favorable al interesado aunque exija una acción por su parte²⁶ para expresar su deseo de no recibir más notificaciones comerciales.

Referente a la protección de los datos personales en los servicios avanzados de telefonía, señalamos, en primer lugar, la supresión en origen, llamada a llamada, de la identificación de la línea llamante

La primera de las facilidades que obliga a ofrecer por los operadores al usuario se centra (artículo 70), en la facilidad de que en cada llamada que realice pueda suprimir la identificación de la línea llamante mediante un procedimiento sencillo y gratuito. Esto es, el derecho del usuario a que no se identifique, o no se presente, al destinatario de la llamada el número de la línea desde la que está realizando la llamada. Se trata de una básica medida de prudencia a los más elementales derechos de protección de la intimidad.

En segundo lugar, haremos referencia a la supresión en origen, por línea, de la identificación de la línea llamante.

La supresión respecto a la identificación en origen de la línea llamante se podrá realizar también en forma automática, sin necesidad de realizar la llamada a llamada, centrándola en la línea desde la que se realiza la llamada, con lo que, repetimos que en forma automática, todas las llamadas que se realicen por esa línea suprimirán la identificación del número telefónico desde el que se llama que, consiguientemente, no aparecerá en el terminal de destino que no identificará, por tanto, desde qué línea se realiza la llamada que entra.

²⁵ Sin cargo alguno y de manera sencilla, indica el apartado 2, del artículo 13 de la Directiva.

²⁶ La de solicitar que no se le vuelva a enviar información comercial a través de ese medio.

Esta facilidad se ofrecerá en forma gratuita a los abonados que podrán solicitarla a intervalos de seis meses en el sentido de activación o desactivación de la facilidad, según corresponda, pudiendo los operadores establecer un precio para las activaciones o desactivaciones que se soliciten en menores intervalos.

Señalaremos la particularidad de que, si el usuario realiza una elección de un operador determinado para realizar su llamada y la selección la realiza mediante un código en el momento de establecer la comunicación, éste código —el de selección de operador— no deberá presentarse en destino.

Tratamos, por último, de la supresión en destino de la línea llamante, y filtrado en destino de llamadas sin identificar.

De igual forma a lo indicado hasta ahora, será posible que el abonado que reciba una llamada pueda suprimir en destino la identificación de la línea llamante mediante un procedimiento sencillo y gratuito.

Respecto al filtrado en destino de llamadas sin identificación cuando se ofrezca en destino la identificación de la línea llamante, cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante y ésta se presente con anterioridad a que se establezca la llamada, el abonado que reciba la llamada deberá tener la posibilidad, mediante un procedimiento sencillo, de rechazar las llamadas entrantes procedentes de usuarios o abonados que hayan suprimido la presentación de la identificación de la línea que origina la llamada.

El artículo 8o. de la Directiva regula esta cuestión refiriéndose expresamente a la posibilidad del usuario de impedir en cada llamada la presentación de la identificación de la línea de origen y la del abonado que origine la llamada a hacerlo por cada línea (apartado 1), la posibilidad del abonado que reciba la llamada de impedir la presentación de la identificación de la línea de origen en las llamadas entrantes (apartado 2), la posibilidad del abonado que reciba una llamada de rechazar las llamadas entrantes procedentes de usuarios o abonados que hayan impedido la presentación de la identificación de la línea en origen (apartado 3) y, por último, la posibilidad al abonado que recibe la llamada de impedir la presentación de la identificación de la línea conectada al usuario que efectúa la llamada (apartado 4).²⁷

²⁷ Aunque pocos efectos tiene en cuanto a protección de datos, queremos resaltar que la Directiva indica, en todos estos casos, que se debe ofrecer la posibilidad que regulan

VI. A MODO DE CONCLUSIÓN

A la luz de la importancia que adquiere la protección de datos, como garantía de una correcta actuación por parte de quien trata los datos y del respeto que puede esperar el titular de los mismos, se hace imprescindible recordar que las comunicaciones electrónicas tienen una repercusión inmediata e importante en este aspecto que redundando directamente en la necesidad de protección del derecho fundamental tratado.

Respecto a Internet, es evidente que no puede representar un vacío jurídico, lo que implica que deba garantizarse la aplicación en toda su extensión tanto de la normativa comunitaria en la materia, como de las normas que regulan en nuestro ordenamiento jurídico la protección de datos.

En algún caso, el uso de las tecnologías de la información y las comunicaciones podría no ser el adecuado y, aun siendo lícito, incidir sobre algún tratamiento que proporcione beneficios directos o indirectos al operador de telecomunicaciones como consecuencia del aprovechamiento de datos o informaciones de las que dispone por una actividad y con unos fines lejanos, o al menos ajenos, al de su actividad principal o, en el otro extremo, beneficiándose los usuarios de las posibilidades que la tecnología les ofrecen para la comisión de actos ilícitos que perjudiquen los derechos e intereses legítimos de los titulares bien sean sobre sus obras u otras producciones, bien sea atacando directa o indirectamente derechos de alta y singular protección como puede ser el derecho fundamental a la protección de datos que ahora analizamos.

Es por ello que se han desarrollado y se recomiendan, incluso desde instancias oficiales, la adopción de medidas tecnológicas que permiten ofrecer una protección a los titulares de derechos frente a acciones que pueden perjudicar sus derechos e intereses legítimos. Se trata de medidas que tienen por objeto ofrecer la protección necesaria, siendo en algunos casos medidas complementarias a las contempladas en la Ley, y que permiten dar respuesta a las necesidades específicas en el entorno electrónico.

mediante “un procedimiento sencillo y gratuito”, a excepción del caso de ofrecer al abonado la posibilidad de rechazar las llamadas entrantes procedentes de usuarios o abonados que hayan impedido la presentación de la identificación de la línea de origen, en el que solamente se exige un procedimiento sencillo, sin hacer mención alguna a la gratuidad o al coste. Distinción o excepción que consideramos de interés.

Al igual que ocurre en el mundo *off-line*, la protección de datos en Internet y, en general, en las comunicaciones electrónicas, se convierte en una obligación para quienes tratan datos de los usuarios y en una garantía para estos últimos. Si bien dicha protección habrá de ser el resultado del equilibrio entre el máximo respeto a las disposiciones legales, recordando que no todos los ordenamientos jurídicos tratan la cuestión de la misma forma, y son diferentes las soluciones tecnológicas que desde la industria del *hardware* y *software* se desarrollen para dar respuestas específicas a esta cuestión.

No cabe duda de que los nuevos servicios que se ofrecen a través de las redes de comunicaciones electrónicas son de gran interés y pueden revolucionar el mercado tradicional o, al menos, modificar la forma de actuar e interrelacionarse en el mismo; pero también resulta evidente que proporciona mayores riesgos a la intimidad de la persona y produce situaciones de indefensión jurídica que, en algunos casos, plantea seriamente su conveniencia.

En muchas ocasiones, gran parte de los problemas se solucionarían con un tratamiento leal de los datos,²⁸ entendido en la forma que lo presenta el considerando 38 de la Directiva General sobre Protección de Datos²⁹ y que se basa en un principio elemental, recogido en las normas, pero que parece más una indicación del sentido común, centrado en una transparente información al titular de los datos que le permita actuar en la forma que considere mejor para sus intereses y en defensa de su intimidad.

Concluiremos indicando que no debemos olvidar que si la eficacia y el progreso son necesarios, nunca deben ser comprados a un precio en el que esté incluido un recorte en las libertades de la persona. Por otro lado, no es conveniente separar, como día a día se va haciendo, tecnología de humanismo. Por el contrario, es conveniente unir ambos términos para lo-

²⁸ En múltiples ocasiones acudimos a la recomendación de la lealtad de los tratamientos; incluso se presentan casos en los que las dudas sobre la licitud de algún tratamiento de datos de carácter personal, o la incertidumbre que conlleva distintas y distantes interpretaciones de las normas creando la inseguridad jurídica que, a veces, llega a frenar el mercado y el desarrollo, se solucionan con recomendaciones de lealtad en el tratamiento.

²⁹ El considerando 38 de la que denominamos Directiva General sobre Protección de Datos —Directiva 95/46/CE—, indica que “el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención”.

grar una interrelación que justifique el progreso de la sociedad junto a su característica básica: el carácter humanitario de la persona. El desarrollo tecnológico debe ir así avanzando, en paralelo, haciendo siempre referencia al bien del género humano, en lo que podemos llamar el “humanismo tecnológico”.³⁰

³⁰ De igual forma, profundizando en el tema, me expreso en mi trabajo “La uniformidad de las leyes de datos: una necesidad”, *Revista de la Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCJET)*, Madrid, núm. 24, 1987. pp. 36 y ss.