LA SEGURIDAD JURÍDICA EN EL ENTORNO DIGITAL

LEGAL CERTAINTY IN THE DIGITAL ENVIRONMENT

RAFAEL GARCÍA DEL POYO[1]

I. INTRODUCCIÓN

Esta contribución pretende presentar algunas consideraciones jurídicas en relación con la seguridad de las actividades económicas que se realizan en los entornos digitales, y más en concreto, en el entorno de Internet. Internet se ha convertido en una herramienta global, que pone en contacto a operadores digitales localizados en muy diversas partes del planeta. Sin embargo, el derecho que regula Internet es, en primer lugar, limitado y, en segundo lugar, marcadamente local. Por ello, resulta conveniente que los operadores conozcan las limitaciones legales que afectan a las actividades que se desarrollan en los entornos digitales.

Dada la amplitud del tema y con el objeto de arrojar luz a esta realidad que hoy día vivimos, hemos tomado como ejemplo aquellas materias que por su actualidad y por afectar tanto a personas físicas como jurídicas pudieran resultar de mayor interés para el lector. Así mismo, hemos tratado de ofrecer una perspectiva jurídica general sobre aquellos servicios o herramientas que, por su exponencial crecimiento, se han introducido en nuestras vidas diarias tanto doméstica y empresarial –prácticamente- sin apenas ser conscientes. Más en concreto, hemos intentado analizar los problemas jurídicos más comunes que se generan en la utilización de estas herramientas, al tiempo que hemos identificado aquellas soluciones que ofrece la legislación vigente en nuestro país en materia de derecho de las tecnologías de la información y de las telecomunicaciones.

Como hemos anticipado, las concretas materias que hemos elegido abordar a título meramente ejemplificativo son: el fenómeno en expansión de los servicios de *cloud computing;* las novedades en la regulación del uso de las *cookies*; la problemática jurídica que plantea la utilización de herramientas de *inteligencia económica;* y la seguridad en la red y los operadores de mensajería instantánea.

[1] Abogado. Socio de OSBORNE CLARKE.

Y el análisis jurídico que vamos a realizar lo basaremos esencialmente en aquel derecho positivo vigente en nuestro país que resulta aplicable en la rama del, ahora denominado por muchos, derecho digital:

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de los datos de carácter personal ("LOPD") y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal ("RDLOPD").
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico ("LSSI").
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias ("TRLGDCU").
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia ("LPI").

II. *CLOUD COMPUTING*

Los servicios de *cloud computing*, suponen el surgimiento de una original herramienta que ofrece soluciones a distintos problemas a los que se enfrentan las empresas, especialmente las grandes corporaciones y las empresas que basan su actividad en la red. Mediante esta herramienta se posibilita a los usuarios la capacidad de acceder a un catálogo de servicios estandarizados que sirven para responder a las necesidades de los individuos y de las empresas de una forma flexible y adaptativa.

Las principales ventajas que ofrece la nube son variadas, el hecho de que la empresa –en principio- no va a verse en la necesidad de instalar ningún hardware adicional y, por lo tanto, se requerirá de una inversión inicial menor de la que debería haberse realizado en el pasado para obtener unos rendimientos productivos similares, se producen mayores compatibilidades y capacidades de integración con el resto de aplicaciones informáticas, proporcionando una mayor capacidad de recuperación en caso de desastre y reduciendo los tiempos de inactividad del sistema. Otra de las grandes ventajas de la nubes es que se permite en paralelo por parte del cliente un seguimiento continuo de su actividad, lo que contribuye a realizar una gestión transparente que repercute en un mayor "bienestar contractual" de las partes. Esto supone una gran novedad respecto a los servicios tradicionales de almacenamiento, en los cuales la gestión era más opaca.

El grupo de trabajo del artículo 29 ("WP29") en su Opinión 05/2012 ya advirtió acerca de los riesgos para la confidencialidad, disponibilidad, integridad, y portabilidad de los datos, ya que a través del *cloud computing* se puede llegar a poner en peligro la libertad de disposición de la información de las empresas, argumento este especialmente digno de consideración si aceptamos que en la sociedad de la información el activo más valioso de una compañía es precisamente su información.

En este sentido, el grupo de trabajo advierte acerca de los siguientes riesgos fundamentales:

- Disminución de disponibilidad debido a la merma en la interoperabilidad (cautivos de un sólo proveedor): dificultad para la transferencia de datos entre diferentes proveedores de nubes o con otras entidades que utilizan sistemas diferentes de nubes.
- Disminución de la integridad de los sistemas por operar con recursos compartidos: Las infraestructuras de las nubes se realizan a través de sistemas y recursos compartidos.
- Disminución de confidencialidad: Es el riesgo que entraña que los servidores donde se aloje la información de la nube no se encuentren dentro del ámbito territorial de la UE y por lo tanto no cumplan con la normativa de seguridad que exige la UE en materia de protección de datos.
- Disminución de la capacidad de control debido a la complejidad de las dinámicas de la externalización de los servicios.

De este modo se deduce que mediante el modelo *cloud*, las compañías depositan sus informaciones de negocio más valiosas y los datos personales de los que disponen en manos de terceros, y esta información recorre diferentes nodos de comunicaciones electrónicas para llegar a su destino. Cada uno de ellos y sus respectivos canales de acceso pueden convertirse en un foco permanente de inseguridad y, por esta razón, se deben utilizar protocolos seguros de comunicación de esa información.

Otro riesgo reside en que la velocidad de acceso a la información puede llegar a disminuir drásticamente, debido a la sobrecarga de transmisión de información que requieren este tipo de protocolos lo cual puede llegar a producir un excesivo grado de dependencia, tanto de los proveedores de servicios de *cloud computing* como de los proveedores de acceso a Internet. Incluso, la externalización de los servicios *cloud* puede implicar que la información acabe alojándose en países que no pertenecen a la Unión Europea y, por tanto, se produzca sin las garantías jurídicas que –por ejemplo, en España- se exigen en materia de protección de datos.

Por todo ello, la aplicación y la adecuación al entorno *cloud* de la normativa sobre protección de datos personales actualmente vigente en España se ha convertido en una materia de estudio de especial importancia. En paralelo, también está siendo analizada por parte de diversas autoridades e instituciones nacionales e internacionales. Resulta evidente que en el marco de la prestación de estos "servicios de computación en nube" o de *cloud* se suscitan importantes interrogantes en materia de protección de datos personales, en especial, sobre qué garantías resultan aplicables y cuáles son jurídicamente exigibles.

Para que se produzca una adecuada prestación de servicios en la nube, resulta imprescindible que el prestador de los mismos no sólo tenga acceso a determinada información de la compañía, sino que normalmente conlleva el encargo de su almacenamiento. En ese caso, la ubicación física de la información (incluidos los datos

personales) se traslada desde las instalaciones de la empresa a los servidores del prestador de servicios de *Cloud*. En cualquier caso, el prestador de servicios de *Cloud* será el encargado de velar por la seguridad de la información, por lo que toda empresa que se halle en la tesitura de decidir acerca de contratar unos u otros servicios prestados en la nube y en qué condiciones hacerlo, habrá de tener muy en cuenta un aspecto fundamental: ¿de qué modo se preservará la privacidad de los datos personales y la información de la compañía?

La pérdida de control directo sobre tal información por parte del responsable del fichero comporta en todo caso un riesgo, cuya cobertura debe asegurarse por vía contractual, particularmente, mediante la negociación del contrato que fije las condiciones en que debe prestarse el servicio de *Cloud Computing.*

Como decimos, la forma de entrega de información empresarial a un tercero dependerá del alcance o de las funcionalidades *Cloud* contratadas. Sin embargo, el acceso por parte de un tercero a esa parte de la información de la empresa que constituyen los datos de carácter personal, a nuestro juicio, se enmarca en el supuesto de "Acceso a los datos por cuenta de tercero", contemplado en el artículo 12 de la LOPD. Un acceso a los datos en estas circunstancias no requerirá el consentimiento del afectado (esto es, de la persona cuyos datos fueron recabados) para que el acceso en cuestión se produzca en condiciones de perfecto cumplimiento de la normativa aplicable, pues tal acceso resulta necesario para la prestación de un servicio al responsable del fichero de datos (en este caso, la compañía beneficiaria de los servicios de *Cloud*).

Sin embargo, el hecho de que tal acceso no requiera el consentimiento del afectado no exime de la obligación de firmar un contrato de encargo de tratamiento en el que se establecerán las condiciones en que el tratamiento de los datos tendrá lugar y la finalidad para la que se destinarán los mismos, o alternativamente, se deberán contemplar con detalle las condiciones del encargo en el propio contrato de prestación de servicios de *Cloud*. Del mismo modo, deviene fundamental asegurarse de que el prestador de servicios de *Cloud* pondrá en funcionamiento las medidas de seguridad necesarias para proteger el acceso a los datos en cuestión; medidas de índole técnica y organizativa tendentes a garantizar la seguridad e integridad de los datos, que impidan su alteración, pérdida, tratamiento o acceso no autorizado y que deben ser en todo caso acordes con la naturaleza de los datos que son objeto de tratamiento.

Finalmente, tal y como ya hemos abordado, conviene tener presente que los servicios Cloud se prestan a menudo mediante el traslado de datos personales a servidores que pueden estar ubicados en el extranjero. He aquí otro aspecto importante que debe considerarse en el momento de negociar un contrato de servicios de *Cloud* pues, en función de las condiciones en que tal movimiento internacional de datos vaya a producirse, las implicaciones para las partes serán variadas. Así, en aquellos casos en los que la transferencia internacional de datos tenga como destino un Estado Miembro de la Unión Europea, o un Estado respecto del cual la Comisión Europea haya declarado que garantiza un nivel de protección adecuado, no será necesaria la expresa autorización

del Director de la Agencia Española de Protección de Datos ("AEPD") (sin perjuicio de la notificación preceptiva a la misma por la cual se ponga en su conocimiento que se va a producir esa transferencia internacional de datos). En otros supuestos, resultará preceptiva la autorización del Director de la AEPD y la comunicación a la misma respecto de tal transferencia de datos.

III. *COOKIES*

Las denominadas "*cookies*" son programas informáticos que almacenan información en el equipo del usuario y que permiten que se acceda a la misma. Se trata en definitiva de dispositivos que facilitan la navegación por Internet pero cuyo uso puede llegar a desvelar aspectos de la esfera privada de los individuos a los prestadores de servicios.

La novedad introducida en el art. 22.2 de la LSSI, consiste en la exigencia de recabar el consentimiento del usuario en relación con el empleo y uso de archivos o programas denominados como *cookies* en sus equipos. En relación con el uso de las *cookies*, la Unión Europea ha introducido una reforma en su regulación a través de la Directiva 2009/136/CE que viene a modificar lo regulado para el uso de las *cookies* por la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y que ha sido transpuesto recientemente a la legislación nacional por vía de la modificación del artículo 22(2) de la Ley 34/2002 de los Servicios de la Sociedad de la Información y del Comercio Electrónico ("LSSI").

Antes de entrar en el análisis de las recomendaciones que realizan el WP29 y la AEPD, consideramos relevante recordar las categorías que establece la AEPD en su *Guía sobre el uso de las cookies*[2] ("Guía"), cuyas orientaciones no pretenden ofrecer una solución general y uniforme para el cumplimiento de la Ley sino que deben servir de guía para que las entidades afectadas reflexionen y adopten decisiones sobre la solución más adecuada a sus intereses y modelo de negocio:

1. Tipos de *cookies* según quien sea la entidad que gestione el equipo o dominio desde donde se envían las *cookies* y trate los datos que se obtengan, podemos distinguir:

- *Cookies* propias: son aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario.
- *Cookies* de tercero: son aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las *cookies*. En el caso de que las *cookies* sean instaladas desde un equipo o dominio gestionado por el propio editor pero la información que se recoja

[2] El 29 de abril de 2013, la Agencia Española de Protección de Datos (AEPD) y las asociaciones Adigital, Autocontrol e IAB Spain presentaron la primera guía en Europa elaborada conjuntamente por la autoridad de protección de datos y los representantes de la industria. La Guía sobre el uso de las cookies recoge las orientaciones, garantías y obligaciones que la industria se compromete a difundir y aplicar para adaptar la instalación de este tipo de archivos a la legislación vigente.

mediante éstas sea gestionada por un tercero, no pueden ser consideradas como *cookies* propias.

2. Tipos de *cookies* según el plazo de tiempo que permanecen activadas en el equipo terminal podemos distinguir:

- *Cookies* de sesión: son un tipo de *cookies* diseñadas para recabar y almacenar datos mientras el usuario accede a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (p.e. una lista de productos adquiridos).
- *Cookies* persistentes: son un tipo de *cookies* en el que los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.

3. Tipos de *cookies* según la finalidad para la que se traten los datos obtenidos a través de las *cookies*, podemos distinguir entre:

- *Cookies* técnicas: son aquéllas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan como, por ejemplo, controlar el tráfico y la comunicación de datos, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, realizar la solicitud de inscripción o participación en un evento, utilizar elementos de seguridad durante la navegación, almacenar contenidos para la difusión de videos o sonido o compartir contenidos a través de redes sociales.
- *Cookies* de personalización: son aquéllas que permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el terminal del usuario como por ejemplo serian el idioma, el tipo de navegador a través del cual accede al servicio, la configuración regional desde donde accede al servicio, etc.
- *Cookies* de análisis: son aquéllas que permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de *cookies* se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio. Respecto al tratamiento de datos recabados a través de las *cookies* de análisis, el grupo de trabajo del articulo 29 ha manifestado que, a pesar de que no están exentas del deber de obtener un consentimiento informado para su uso, es poco probable que representen un riesgo para la privacidad de los usuarios siempre que se trate de *cookies* de primera parte, que traten datos agregados con una finalidad estrictamente estadística, que se facilite información sobre sus uso y se incluya la posibilidad de que los usuarios manifiesten su negativa sobre su utilización.

- *Cookies* publicitarias: son aquéllas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado en base a criterios como el contenido editado o la frecuencia en la que se muestran los anuncios.
- *Cookies* de publicidad comportamental: son aquéllas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado. Estas *cookies* almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.

El uso de las *cookies* supone una alternativa a los formularios como medio de obtención de datos personales a través de la red. Antes de la reforma, la LSSI sólo requería que los proveedores de servicios facilitaran cierta información al usuario. La nueva regulación dada en España respecto al uso de las *cookies* establece que los proveedores de servicios de la sociedad de la información podrán instalar *cookies* en los dispositivos de los usuarios siempre que los usuarios hayan otorgado su consentimiento informado al efecto. En particular, la nueva regulación establece dos medios alternativos para la obtención del consentimiento del usuario válidamente:

- Que el usuario consienta previamente, una vez éste haya sido completa y adecuadamente informado sobre el uso de las *cookies*, en particular sobre las finalidades del tratamiento de los datos de carácter personal del usuario de acuerdo con lo previsto en la LOPD;
- Que el usuario dé su consentimiento por medio de un acto expreso con respecto a la configuración de su ordenador u otra aplicación, durante su instalación o actualización, o cuando quiera que sea posible técnicamente y eficiente hacerlo.

No obstante, y contrario a lo que se su suele afirmar sobre esta materia, la citada legislación no requiere un mecanismo de "opt-in" o consentimiento expreso, si viene es cierto que no da una solución clara respecto a la forma de obtención del consentimiento. El WP29 emitió el día 7 de junio de 2012 una Opinión por la cual se establecen directrices sobre el uso de las *cookies*, en particular se establecen las categorías de *cookies* que se encuentran exentas de la obligación de obtener el consentimiento informado del usuario. Se establecen cuatro categorías distintas de *cookies*:

- *Cookies* cuyo uso es estrictamente necesario (son estrictamente necesarios para permitir al usuario navegar por el sitio web y utilizar los distintos servicios).
- *Cookies* para el funcionamiento del sitio web (limitados al funcionamiento y mejora del sitio web).
- *Cookies* de funcionalidad (permiten recordar las elecciones del usuario y facilitar otro tipo de información local).
- *Cookies* de publicidad o de *target* (permiten distinguir los hábitos de

navegación del usuario).

Asimismo, la AEPD en su Guía incluye directrices, garantías y obligaciones que las empresas del sector se comprometen a aplicar para adaptar el uso de este tipo de archivos por parte de las empresas al marco legislativo vigente en España. Las soluciones recogidas en la Guía ofrecen recomendaciones básicas que ayuden a cumplir con las obligaciones establecidas por el artículo 22.2 LSSI.

Así, en su Guía, la AEPD recoge lo establecido por el WP29 en cuanto a los tipos de *cookies* que quedan exceptuadas de la obligación de recabar el consentimiento:

- *Cookies* de entrada del usuario.
- *Cookies* de autenticación o identificación del usuario (únicamente de sesión).
- *Cookies* de seguridad del usuario.
- *Cookies* de sesión de reproductor multimedia.
- *Cookies* de sesión para equilibrar la carga.
- *Cookies* de personalización de la interfaz del usuario.
- *Cookies* de complemento (plug-in) para intercambiar contenidos sociales.

Las normas establecidas en la Guía pretenden asegurar que los usuarios puedan decidir si prestan su consentimiento o no a la instalación de *cookies* en sus dispositivos, con información clara y completa acerca de cuáles son los datos que se obtendrán realmente, quién llevará a cabo el tratamiento y a qué finalidades se destinarán. De esta manera, como para la instalación y uso de las *cookies* por parte de las compañías es necesario obtener el consentimiento del usuario, se puede considerar consentimiento informado. Este consentimiento sólo se puede obtener a través de fórmulas expresas, como rellenando una casilla o infiriéndolo de alguna acción del usuario. Como consecuencia, para que el consentimiento sea válido, es necesario que éste sea expresado de alguna manera ya que la mera inactividad del usuario no puede ser considerada como consentimiento otorgado.

La Guía ofrece varias posibilidades para cumplir con las dos obligaciones legales impuestas por la legislación: el deber de informar al usuario y obtener su consentimiento. En cuanto a la obligación legal de informar, los proveedores de servicios deberán proporcionar una información clara y completa acerca del uso de *cookies* que pretenden. En este sentido, la Guía recomienda un sistema de información *por capas*, en el que se muestre la información más esencial en la primera capa en el momento de acceder a la página web o la aplicación y se complete en una segunda capa mediante una página que proporcione información adicional sobre las *cookies* usadas.

La información proporcionada al usuario deberá ser suficientemente completa como para permitir a los usuarios entender la finalidad del uso de las *cookies*, el uso real que se hace y a quién se transferirán los datos, en su caso. A este respecto, y dado que las compañías deben asumir que el conocimiento de los usuarios sobre el uso de las *cookies* y su gestión es muy limitado, la Guía recomienda a éstas tener en cuenta el tipo de usuario que realmente navega en su página web o utiliza una cierta aplicación para

adaptar el lenguaje y el contenido al concreto nivel de dominio del usuario. Cuanto menor es el nivel de dominio del usuario, más simple ha de ser el lenguaje empleado para informarle con el fin de evitar que la terminología técnica contenida en la información facilitada resulte incomprensible.

Asimismo, la Guía incluye directrices respecto a la accesibilidad y visibilidad de la información que debe ser facilitada por las compañías. Aunque la Guía no establece normas estrictas sobre dónde se ha de colocar la información, sí especifica que el *link* que redirige a esa información debe estar situado en zonas que realmente capten la atención del usuario.

Por último, la Guía incluye el derecho de los usuarios a recibir información sobre cómo deshabilitar o eliminar las *cookies* y cómo revocar el consentimiento previamente dado al uso de las mismas.

Dadas las muchas dificultades que plantea el uso de *cookies*, la Guía no pretende proporcionar unas normas de cumplimiento uniformes y generales sino directrices para las entidades afectadas que les permita adoptar la solución que mejor se adapta a sus intereses y su modelo de negocio. La AEPD recomienda a las entidades afectadas llevar a cabo una revisión, internamente o con ayuda de asociaciones o entidades especializadas.

La publicación de esta Guía sirvió para que los proveedores de servicios de la sociedad de la información se pusieran al día en cuanto a las novedades en el ámbito del uso de las *cookies* y evitaran las sanciones que establece la LSSI que van desde 30.001 a 150.000 euros.

IV. INTELIGENCIA ECONÓMICA

Se define la inteligencia económica como el control y la protección de la información estratégica pertinente para todos los agentes económicos. Este tipo de inteligencia se realiza mediante la recogida, el análisis y la difusión de la información económica estratégica obtenida con la finalidad de mejorar la competitividad de una determinada organización.

Algunos afirman que el concepto de Inteligencia Económica simplemente constituye la adaptación francesa del concepto de "*business intelligence*" de los británicos y de la "*competitive intelligence*" de los norteamericanos y que podría resumirse en una "forma de buen gobierno cuyo objeto es el dominio de información estratégica".

El escándalo desatado por el Proyecto PRISM en Estados Unidos ha provocado diversas reacciones de temor ante la preocupación de que algo así sea (lícitamente) posible en Europa. El controvertido Proyecto PRISM recibe su legitimidad de la no menos controvertida ley estadounidense FISA ('*Foreign Intelligence Surveillance Act*'). La Ley FISA establece procedimientos para la vigilancia tanto física como electrónica y

la recogida de información procedente de agencias de inteligencia extranjeras.

Al parecer, tal y como se ha dado a conocer, la NSA ha obtenido datos de llamadas telefónicas y comunicaciones electrónicas también de ciudadanos estadounidenses y, aunque estos datos obtenidos no suelen contener referencias a la identidad del usuario ni al contenido de las comunicaciones, sí se han analizado aquellos datos que se van generando al realizar dichas comunicaciones, esto es, los metadatos. Los metadatos son "datos sobre los datos" y por ello pueden definirse de forma muy básica como aquella información que se genera cuando usamos medios y tecnologías de la información para comunicarnos. Entre estos datos podemos encontrar la fecha y la localización de una llamada o la dirección de correo electrónico del emisor o del receptor de un mensaje.

Esta noticia ha generado reacciones por parte de grandes compañías de la comunicación electrónica. En líneas generales, algunas de estas compañías han negado públicamente conocer la mera existencia del programa PRISM, así como haber ofrecido acceso directo a sus servidores a cualquier agencia estatal estadounidense. Otras de estas compañías se remiten a lo establecido en la normativa sobre protección de datos, en tanto que es necesaria una orden judicial para acceder a los ficheros que contienen información de una empresa.

Tras este somero análisis de la polémica suscitada, la reacción del Supervisor Europeo de Protección de Datos a las potenciales consecuencias para los ciudadanos europeos del análisis realizado por la NSA no se ha hecho esperar. El pasado día 10 de junio de 2013 el Supervisor emitió una declaración en la que expresaba su preocupación ante los acontecimientos y aseguraba que se trataría el asunto en una futura cumbre entre autoridades estadounidenses y europeas.

En todo caso, un análisis de similares características realizado en la Unión Europea debería tomar su base en las legislaciones nacionales de cada Estado miembro, ya que en la Unión se ha legislado la materia a través de varias directivas que han sido transpuestas en los ordenamientos jurídicos nacionales. Así en España, en la Ley Orgánica 15/1999 de protección de datos (LOPD), podemos encontrar referencias a ciertas excepciones en favor de las autoridades del Estado. En su artículo 11, se exime del siempre requerido consentimiento del interesado a aquellas comunicaciones de datos que tengan por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas. La razón detrás de esta dispensa del primordial requisito del consentimiento es el potencial "interés público" que podría derivarse de conocer esos datos.

Por otro lado, la Directiva 2004/26/CE 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 su norma de transposición en España, la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, establecen un sistema por el cual se obliga a los operadores que presten servicios de comunicación electrónica

disponibles al público o que exploten redes públicas de comunicaciones a conservar los datos generados o tratados en el marco de la prestación de servicios y a cederlos a las autoridades facultadas que los requieran previa autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves. En el artículo 3 de esta ley se puede comprobar que entre los datos de obligada conservación se encuentran los metadatos que surgen durante la prestación de servicios entre operador y usuario. El período de conservación de los datos se limita a 12 meses, con posibilidad ser ampliado a 2 años o limitado a 6 meses. Entre las autoridades facultadas a analizar esta información se encuentran las Fuerzas y Cuerpos de Seguridad del Estado, el personal aduanero, cuando ejerza funciones de policía judicial, y el personal del Centro Nacional de Inteligencia.

Si volvemos de nuevo al concepto general de inteligencia económica, como juristas debemos examinar las consecuencias que pueden derivarse por la utilización de estos sistemas –muy especialmente- en el ámbito de la protección de datos de carácter personal. Y ello, porque debe tenerse en cuenta que las herramientas de inteligencia económica utilizan la información existente en la empresa para la creación de conocimiento y entre esos datos pueden encontrarse incluidos datos de carácter personal.

A la luz de la LOPD, se considera dato personal cualquier información concerniente a personas físicas identificadas o identificables. En este sentido, desde el momento en el que las herramientas de inteligencia económica capten, utilicen, o traten de cualquier manera datos o información referente a personas físicas identificadas o identificables deberán respetar lo establecido en la LOPD y en su normativa de desarrollo.

Principalmente, debe tenerse en cuenta que el tratamiento de datos de carácter personal se asienta sobre el principio de calidad y finalidad de los datos personales. Así, el artículo 4 de la LOPD establece que los datos personales solo podrán ser tratados en la medida que sean adecuados, pertinentes y no excesivos para las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Este principio toma especial relevancia en la utilización de los sistemas de inteligencia económica por parte de cualquier compañía, principalmente en lo referente al tratamiento de datos personales de los empleados de la compañía.

El tratamiento de datos de carácter personal debe realizarse con motivo de una concreta finalidad, que deberá ser informada al individuo en virtud del artículo 5 de la LOPD. En este sentido, las compañías únicamente podrán tratar los datos con motivo del desarrollo de dicha finalidad. Así, tomando como ejemplo el tratamiento de datos de los empleados de una compañía, no podrán utilizarse los sistemas de inteligencia económica para tomar decisiones que vayan más allá de la mera gestión, desarrollo o control de la relación laboral que mantienen con el empleado. Por lo tanto, en el caso de que se utilicen estas herramientas para la toma de decisiones que puedan ser consideradas como discriminatorias, más allá de las implicaciones que pueda tener en el ámbito laboral, se estará produciendo un tratamiento ilegítimo de datos personales que

podría conllevar una sanción por parte de la AEPD.

Otro de los aspectos más relevantes que deben tomarse en consideración en la implantación de este tipo de herramientas son los accesos que se pueden realizar a la misma por compañías de un mismo grupo empresarial. Así, resulta frecuente que con la finalidad de crear las mayores sinergias posibles dentro de un grupo, se instale una única aplicación informática en el mismo donde todas las sociedades del grupo vuelcan su información –de carácter personal o no- con la finalidad de que pueda ser utilizada por el resto de compañías del grupo. De esta manera, en el caso de que la información que faciliten las compañías de un grupo empresarial contenga datos de carácter personal, se estará produciendo una cesión de datos personales al resto de sociedades del grupo que requerirá, en la mayoría de las ocasiones, del consentimiento de los interesados.

En este sentido, cabe destacar que las herramientas de inteligencia de negocio han favorecido el desplazamiento internacional de información empresarial. Como no podría ser de otra manera, la utilización en el mundo empresarial moderno de información relacionada con personas físicas -datos de carácter personal- relativa a clientes, proveedores, empleados y potenciales clientes, entre otros, es objeto de un constante tratamiento que en multitud de ocasiones supone el traslado, físico o lógico, de la información de uno a otro país, esto es, de una a otra jurisdicción, e implica la consiguiente "intervención" por parte de las autoridades -tanto nacionales como europeas- competentes en la materia.

La normativa europea referente al tratamiento de datos de carácter personal ha querido regular expresamente estas comunicaciones internacionales de datos personales y en tal sentido se pronuncian los artículos 25 y ss. de la Directiva 95/46/EC, de 24 de octubre de 1995, del Parlamento Europeo y del Consejo, 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.

Del mismo modo, en su transposición de la citada directiva, la legislación española sobre protección de datos dedica los artículos 33 y 34 de la LOPD a regular las transferencias internacionales de datos, bien sean éstas destinadas a países de la Unión Europea o bien lo sean a países ubicados fuera del territorio de la Unión Europea.

En este mismo sentido, existe en España una Instrucción de la AEPD, la Instrucción número 1/2000, de 1 de diciembre de 2000, que viene a aclarar el contenido de estos artículos de la LOPD y que está específicamente orientada a la reglamentación de dichas transferencias internacionales de datos.

Esta Instrucción 1/2000 define como transferencias internacionales de datos personales "toda transmisión de los mismos fuera del territorio español", por lo que se engloban en este concepto de transferencia internacional tanto aquellas en las que se produce una comunicación de datos a un tercero para que éste actúe por cuenta propia, decidiendo sobre la finalidad del tratamiento en el sentido de lo dispuesto en el artículo

11 LOPD, como aquellas que, sin constituir stricto sensu "comunicación" según lo contemplado en el artículo 11 LOPD, son transmisiones de datos a terceros para que ellos actúen como encargados de tratamiento en el ámbito de la prestación de un servicio, según lo dispuesto en el artículo 12 LOPD.

A los efectos de comprender mejor la legislación española sobre protección de datos personales en lo que respecta específicamente al movimiento internacional de datos, hemos de poner de manifiesto, en primer lugar, que la LOPD y la Instrucción 1/2000 establecen como principio general la prohibición de realizar transferencias de datos personales destinadas a países que no ofrezcan un nivel de protección jurídica equiparable al establecido por la legislación española para el tratamiento de los datos personales.

Aparte de la excepción ya mencionada y que hace referencia a la equiparación del nivel de protección jurídica otorgada en determinados países a los datos de carácter personal, esta prohibición genérica no va a resultar aplicable en ciertos supuestos contemplados en la normativa vigente (por ejemplo, cuando se ha obtenido el consentimiento expreso de afectado). Asimismo esta prohibición también puede exceptuarse mediante la obtención de la previa autorización del Director de la AEPD a la transferencia internacional de datos que se pretenda efectuar. El Director otorgará dicha autorización si el transmitente y el destinatario de los datos suscriben un contrato en el que se establezcan las garantías exigidas por la referida Instrucción 1/2000 o si han firmado un acuerdo que contiene las cláusulas tipo recogidas en la Decisión de la Comisión 2001/497/CE, de 15 de junio de 2001 para cesión de datos, recientemente modificada por la Decisión de la Comisión de 17 de diciembre de 2004, o las contenidas en la Decisión 2002/16/CE, de 27 de diciembre de 2001 para prestaciones de servicios (o lo que es lo mismo, para encargados del tratamiento).

La experiencia que hemos acumulado, especialmente en los últimos años, nos aconseja como la opción más segura y eficaz el procurar la firma de acuerdos o contratos entre empresas que contengan las mencionadas "cláusulas tipo".

Respecto de los países que ofrecen un nivel de protección jurídica a los datos personales equiparable al contemplado en la Directiva Europea (y, por tanto, al establecido en la legislación española), si bien no será precisa la autorización del Director de la AEPD para llevar a cabo la transferencia internacional, sí que deberá contemplarse la notificación de la misma en el correspondiente formulario de inscripción del fichero ante el Registro General de la AEPD.

En conclusión, el régimen jurídico que puede resultar aplicable a las transferencias internacionales es variopinto y su autorización va a resultar más o menos complicada en función del país de destino y las circunstancias específicas que concurran en cada supuesto. Precisamente por ello resulta esencial que una empresa que pretenda transferir o permitir el acceso remoto a los datos de carácter personal de los que es responsable, analice con detenimiento y con carácter previo a su exportación, todos los requisitos que la normativa le impone cumplir, que sopese en su conjunto el esfuerzo y

los recursos humanos y materiales que la transferencia conlleva y que los compare con los potenciales beneficios que puedan resultar de dicha exportación de datos.

Por otro lado, y volviendo a la fase en la que se estudia la posible adquisición de una herramienta de inteligencia económica, otro de las circunstancias que el adquirente debe tomar en consideración a la hora de elegir la concreta herramienta que implementará en su compañía, es si dicha aplicación será capaz de soportar las medidas de seguridad que la normativa existente en materia de protección de datos obliga a implementar en los ficheros automatizados que contengan dicho tipo de información.

El RDLOPD regula las concretas medidas de seguridad que deberán aplicarse a los ficheros que contengan información de carácter personal. Así, en función del tipo de información que se incluyan en los ficheros, las aplicaciones que las soportan deberán ser capaces de soportar las medidas de seguridad de nivel básico, medio o alto que dichas normas establecen.

En este sentido, la disposición adicional única del referido Real Decreto exige que los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en este reglamento.

A modo de conclusión, podemos decir que son numerosas las previsiones legales que cualquier organización (pública o privada) adquirente de herramientas de inteligencia económica debe tener en cuenta en el momento en el que se adquiere y negocia su adquisición, siendo fundamental el asesoramiento de un profesional en la materia que defienda sus intereses ante el productor o licenciante del software.

Una vez analizado el mundo de las herramientas de inteligencia económica desde una perspectiva de protección de datos, conviene ahora destacar las contingencias más comunes que suelen tener lugar desde un punto de vista de derecho de la propiedad intelectual.

Los derechos de propiedad intelectual se dividen en derechos morales y derechos económicos o patrimoniales. Los derechos morales son irrenunciables e inalienables y, por lo tanto, acompañan al autor durante toda su vida y a sus herederos o causahabientes al fallecimiento de aquellos. Sin embargo, los derechos patrimoniales sí son transmisibles. De esta manera, el creador de un software o programa de ordenador tiene la facultad de ceder la explotación del mismo o de permitir su uso mediante licencias a terceros a cambio de una compensación económica. No obstante, los contratos donde se regulan los términos en los cuales un tercero puede utilizar un determinado software suelen no determinar todos los aspectos necesarios para regular específicamente el uso que dicho tercero puede dar al software.

Así, en lo que respecta a los derechos de propiedad intelectual, en caso de que no se regulen específicamente en el contrato pueden surgir contingencias en diferentes ámbitos tales como el (i) la extensión territorial y temporal en la utilización del

software, (ii) las posibilidades de utilización del software por un licenciatario del mismo o (iii) la implantación de las herramientas en las distintas sociedades que forman parte de un grupo empresarial.

En caso de que el contrato donde se licencia el software no contenga expresamente determinadas limitaciones al ámbito de la licencia o no describa detalladamente la extensión de la misma, dichas limitaciones o extensiones podrán igualmente tenerse por determinadas por voluntad presunta de las partes. No obstante, dichas presunciones pueden no beneficiar al licenciatario del software y, por lo tanto resulta fundamental "cerrar" la licencia de uso de software lo máximo posible a los efectos de que no quede duda alguna sobre su alcance, y en algunos casos, modificar la misma con la finalidad de que se adapte a las concretas necesidades del licenciatario.

i) Duración y ámbito de aplicación de la licencia

Se establece en el artículo 43.2 de la LPI que "la falta de mención del tiempo limita la transmisión a cinco años y la del ámbito territorial al país en el que se realice la cesión." De esta manera si el contrato de adquisición de la herramienta no contuviese disposición alguna en materia de duración y ámbito territorial de las licencias otorgadas, las mismas deberán entenderse concedidas por un plazo de 5 años y restringidas al territorio español.

No obstante lo anterior, con referencia a la duración de la licencia nos encontramos con un primer problema ya que el referido artículo también establece que "Si no se expresan específicamente y de modo concreto las modalidades de explotación de la obra, la cesión quedará limitada a aquella que se deduzca necesariamente del propio contrato y sea indispensable para cumplir la finalidad del mismo". Por lo tanto, siendo que el software debe atender a la finalidad para la que se licencie, nos encontramos que en el caso de que el plazo de utilización lógica del software fuese superior a 5 años, no resultaría claro el plazo por el cual se habría concedido la licencia de software, pudiendo resultar la situación en una disputa entre las partes.

ii) Posibilidades de utilización del software por un licenciatario del mismo: el mantenimiento evolutivo y el manteniendo correctivo.

La implantación de sistemas de inteligencia económica por parte de las organizaciones puede requerir un proceso de adaptación/modificación del mismo para la adecuación de la herramienta al modelo de gestión del negocio de dicha empresa o puede resultar necesario que el mismo se adapte a las necesidades del mercado. De aquí surgen dos nuevos conceptos muy ligados entre sí pero diferentes en su tratamiento: el mantenimiento correctivo y el mantenimiento evolutivo del software.

No es nuevo el caso en el que después de un importante desembolso económico por parte de una compañía para la adquisición de una herramienta de software, la misma no se adapta a sus actuales sistemas de gestión de negocio o que se dé el supuesto de que la herramienta tuviese errores o defectos difícilmente conocibles en el momento de

la firma del contrato. Estos dos supuestos engloban lo que es conocido como el mantenimiento correctivo del software.

Por otro lado, los continuos avances existentes en el sector del software llevan a que las herramientas queden obsoletas rápidamente, por lo que en numerosas ocasiones resulta necesaria una nueva versión del software. Estos supuestos hacen referencia a la necesidad de que la adquisición del software se acompañe de un mantenimiento evolutivo del mismo.

Sobre este particular, la pregunta que nos hacemos es ¿está el licenciatario facultado para proceder a la corrección y/o modificación del software? Sobre este respecto, el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, estipula en su artículo 100 que salvo que exista una disposición contractual en contrario, el usuario de una herramienta de software podrá llevar a cabo la reproducción o transformación del mismo con el fin de poder seguir usando el mismo con arreglo a su finalidad propuesta.

No obstante lo anterior, el creador de una herramienta de software, ante el temor de perder su "facultad de control" sobre el software si terceros llevan a cabo la modificación del mismo, suelen incluir en los contratos cláusulas que impiden al licenciatario del software o a cualquier otro tercero llevar a cabo modificaciones o transformaciones de éste. Así, en el caso de que no se cuente con la autorización del titular de los derechos de explotación del programa, para llevar a cabo la modificación del software suelen establecerse en los contratos cláusulas por la cuales decaerá, en su caso, la garantía del software o el establecimiento de cláusulas de exoneración de responsabilidad por parte de la empresa titular de los derechos de explotación.

En cualquier caso, como puede apreciarse, especialmente teniendo en cuanta que este tipo de cláusulas pueden ser negociadas en el momento de adquisición de la herramienta, resulta fundamental contar con la ayuda de un especialista en este tipo de contratos para lograr que estas herramientas no queden vacías de contenido.

Pero no sólo debemos fijarnos en las implicaciones relativas al mantenimiento correctivo sino también en aquéllas referentes al mantenimiento evolutivo de las herramientas. Así, cuando se negocia el mantenimiento evolutivo del software con el proveedor del mismo, debe tomarse en consideración que resulta frecuente que el proveedor de la herramienta utilice una terminología diferente según el alcance de las modificaciones que se han integrado, esto es, si afectan o no al código fuente, o si implican o no nuevas funcionalidades. En consecuencia, resulta fundamental incluir en el contrato los términos precisos que hagan referencia a las obligaciones o potestades de las partes en relación con las versiones del programa.

Sin ánimo de extendernos en este respecto, resulta frecuente que los proveedores del software no se comprometan en el contrato a facilitar versiones del mismo sino que hagan referencia en el contrato a la posibilidad de facilitar dichas versiones. Esto es,

establecen en el contrato el suministro de versiones como una prerrogativa exclusiva del proveedor pero no como una obligación de éste. Por ello, resulta recomendable que el adquirente de este tipo de programas, se encuentre facultado en el contrato a exigir del proveedor de software, una vez adquirido el programa, cualquier modificación que se produzca con posterioridad a la adquisición del programa de ordenador.

Otras cuestiones prácticas que deben tenerse en cuenta a la hora de negociación de este tipo de modificaciones del software son las relativas a la parte encargada de la instalación de la nueva versión, el compromiso del proveedor de que la instalación de las nuevas versiones no afectará a la que se venía utilizando y a las modificaciones incorporadas en la misma o el plazo temporal en el que se obliga a facilitar versiones.

iii) Utilización de la herramienta por distintas sociedades de un grupo empresarial

Otro de los aspectos que deben tenerse en consideración a la hora de adquirir una herramienta de inteligencia económica es la posibilidad de que una vez adquirida la licencia de software por parte de la empresa matriz de un grupo empresarial, se pretendiese la implantación del software en las demás sociedades del grupo.

Sobre este particular, establece el artículo 99 de la LPI que "cuando se produzca la cesión del derecho de uso de un programa de ordenador, se entenderá, salvo prueba en contrario, que dicha cesión tiene carácter no exclusivo e intransferible, presumiéndose, asimismo, que lo es para satisfacer únicamente las necesidades del usuario". En definitiva, esta provisión legal limita las posibilidades de uso del software, que se entiende licenciado a efectos de otorgar cobertura a las necesidades propias del usuario, entendiendo por tal, el licenciatario del software, lo que excluye cualesquiera otras entidades, ya pertenezcan o no, a su grupo empresarial.

Así, para que las filiales de un grupo empresarial puedan beneficiarse del uso que su matriz hace del mismo, es preciso que en el contrato de licencia se establezca tal extremo, esto es, que se determine que se autoriza el uso del software para las actividades propias tanto del licenciatario como de sus filiales.

En uno y otro caso, vemos que se deja un importante margen de negociación a la autonomía de las partes. En este sentido, vemos como la labor de negociación del abogado para la suscripción del acuerdo se antoja fundamental para el desarrollo del mismo.

V. OPERADORES DE MENSAJERÍA INSTANTÁNEA

En este apartado pretendemos analizar un fenómeno que se ha estado y está produciendo en uno de los muchos subsectores del ámbito de los negocios digitales, la mensajería instantánea. La enorme expansión de formas cada vez más novedosas de mensajería instantánea, encuentra su causa en la gratuidad de los servicios que prestan a los usuarios. Este factor resulta de una importancia capital y unido a la expansión de los

denominados "*smart phones*", ha provocado un crecimiento exponencial en el sector aumentando la complejidad en el funcionamiento del mismo, el cual, en bastantes ocasiones, no se produce en las condiciones de seguridad idóneas para el usuario.

En un ámbito como el de la mensajería instantánea, que cada día recibe miles de usuarios nuevos, la seguridad de estos últimos debe encontrarse siempre en la cima de la escala de prioridades del legislador. Y es que las normas que regulan este subsector, en la actualidad, resultan de una gran complejidad en cuanto a su comprensión y aplicación, tanto por lo técnico como por su número.

A primera vista parece claro que, desde que lo primero que hace el usuario al darse de alta en el registro del sitio web o aplicación es proporcionar sus datos personales, estas entidades que operan servicios de mensajería han de cumplir con las obligaciones de este ámbito legislativo, la LOPD y el RDLOPD que la desarrolla. Ello conlleva la inscripción de ficheros, la obtención de los consentimientos preceptivos, la habilitación del ejercicio de los derechos de acceso, el control de las transferencias internacionales… Sin embargo, en cuanto a protección de datos se refiere, la dificultad del regulador estriba en la imposibilidad de aplicar en muchos casos la normativa española o europea, dado que estas vinculan su aplicación a la existencia de un establecimiento en territorio español o europeo y no a la nacionalidad del titular de los datos, que en resumidas cuentas es quien se quiere proteger. Esto provoca que se realicen transferencias internacionales de datos sin control público o que se comercie impunemente con los datos de los usuarios sin que ellos puedan evitarlo.

Sin embargo, con una propuesta de reglamento europeo en materia de protección de datos sobre la mesa, se espera que el legislador interceda para establecer una regulación que mejore las contingencias y riesgos que no evita un marco legislativo cuya piedra angular, el ámbito de aplicación, resulta controvertido e ineficaz.

Por otro lado, al darse de alta en un servicio, uno no sólo pone en riesgo sus datos, sino que también lo que se hace es contratar la prestación de unos servicios con la persona jurídica que hay de tras de la aplicación. En este ámbito la regulación corresponde a la LSSI y al TRLGDCU, que velan por los intereses de los usuarios estableciendo normas protectoras en el ámbito de la contratación electrónica. El problema en cuanto a esta regulación reside en la poca relevancia de la actividad sancionadora hasta la fecha, lo cual hace deseable que se trabaje en este sentido ya que, a pesar de ser una normativa que se aplica por estar dirigidos los servicios a ciudadanos españoles, la sensación general es de impunidad para los operadores de servicios de mensajería instantánea.

Dentro de la LSSI, pero relevante por separado, encontramos un campo en el que sí se ha trabajado más intensamente en cuanto a la regulación, las comunicaciones comerciales por vía electrónica. En los artículos 19 a 22 de la LSSI, se regula este fenómeno. Y es que las comunicaciones comerciales son un ejemplo de cuán necesaria es la actualización de las normas en una rama como es el derecho de las nuevas tecnologías. Si bien la LOPD, salvo alguna reforma, permanece prácticamente

inalterada, la LSSI, que se antoja como el complemento legislativo necesario para aquélla, sí que ha sido actualizada en varios ámbitos entre los que destacan las comunicaciones comerciales por vía electrónica. La reforma que se introdujo estableció el requisito del consentimiento expreso por parte del usuario para recibir comunicaciones comerciales sobre productos por parte de la empresa con la que había contratado o un tercero, cuando aquéllos no fueran similares a los que había contratado. Esto unido a que se habilitó a la AEPD como órgano sancionador para las comunicaciones comerciales, ha resuelto los problemas en cuanto a este fenómeno. Este cambió limitó ampliamente toda la actividad de envío masivo de este tipo de comunicaciones.

VI. CONCLUSIONES

El sector de las Nuevas Tecnologías cambia y se rediseña a un ritmo vertiginoso: el que marca el mercado de la tecnología. Los problemas derivados de la regulación provienen, en su mayor parte, de la velocidad de modernización y actualización de los productos y servicios del sector. Es cierto que el mundo digital se ha convertido en una estructura global, pero el derecho –todavía- no lo es. Por ello, se impone una forma de legislar flexible y adaptada a la volátil realidad de este mercado que ofrezca, entre otros, mecanismos eficaces de resolución de conflictos.

El derecho de las Tecnologías de la Información es desde su origen un cruce de caminos entre prácticamente la totalidad de las ramas principales del derecho. En el entorno digital, los servicios que se ofrecen en el mismo conforman un entorno complejo y global. Sin embargo, las herramientas que nos proporciona el derecho no son globales, no están emitidas por una autoridad global que legisle sobre el mundo de internet, sino que queda regulada de manera parcial y ciertamente localizada. Ello debe conllevar aparejados enormes esfuerzos legislativos para poder dotar a los operadores y a los usuarios de los entornos digitales de un nivel seguridad jurídica deseable y aceptable.

Estamos en un estadio todavía incipiente en cuanto al surgimiento en el mundo jurídico de unos profesionales que ofrezcan sus servicios de una manera global y que puedan aportar soluciones creativas y adecuadas a las necesidades de sus clientes tanto en las áreas regulatorias como las litigiosas. Por ello, en el entorno digital, la necesidad de contar con los servicios de un experto que reúna estas características y que domine la forma en la que el derecho internacional público y privado interactúan con los derechos nacionales se antoja absolutamente fundamental.

Probablemente deberá abordarse en algún momento el debate sobre si las carencias que muestra el derecho como mecanismo para regular las relaciones entre personas, y muy especialmente en los entornos digitales, son fruto de males endémicos, y si es así, deberemos identificar aquellas fórmulas a las que hemos de acudir para solucionar las controversias que también en este entorno surgen entre los seres humanos.

Hoy en día, el entorno digital prácticamente abarca a todos los ámbitos de la actividad humana y la seguridad jurídica de este entorno en un mundo dominado por el poder de la información, resulta vital tanto para la supervivencia y el desarrollo de nuestras empresas como para el mantenimiento de nuestra sociedad dentro de unos niveles adecuados de convivencia. Por ello, es algo en lo que se debe trabajar a diario, de manera continua y con el máximo respeto a los derechos que la normativa vigente contempla en favor los ciudadanos.

BIBLIOGRAFÍA

ESTEBAN NAVARRO, M.A. y NAVARRO BONILLA, D. *Glosario de Inteligencia*, Ministerio de Defensa, Madrid, 2007.
HOWSON, C.: *Business Intelligence. Estrategias para una implementación exitosa*, McGraw Hill, México, 2008.
MARTÍNEZ MARTÍNEZ, R. (coord.), *Derecho y cloud computing*, Civitas Thomson Reuters, 2012.
TRONCOSO REIGADA, A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, 2010.