Anuario Jurídico Villanueva 12 • 2018 Págs. 201 a 238

APROXIMACIÓN INICIAL A DETERMINADAS CUESTIONES RELATIVAS AL ASESORAMIENTO LEGAL EN MATERIA DE COMERCIO ELECTRÓNICO

[Ganador del III Premio de Estudios Jurídicos Villanueva]

■ ■ ■

Juan Saavedra Ortiz

Abogado
jjsaavedra_@yahoo.es

SUMARIO: INTRODUCCIÓN. Problemáticas y particularidades del asesoramiento legal en materia de Comercio Electrónico. Por el ámbito material. Por el ámbito geográfico. Por las particularidades del canal. Por la naturaleza de las cuestiones objeto de análisis. Por el contenido y formato del análisis. El «Entregable». NORMATIVAS MÁS RELEVANTES EN RELACIÓN CON EL COMERCIO ELECTRÓNICO. Normativa de Consumo y Comercio con especial consideración del derecho de desistimiento y la información precontractual. Los Mecanismos Alternativos de Resolución de Conflictos (ADR/ODR) y otras medidas recientes de protección a los consumidores en el ámbito de la Unión Europea («New Deal for Consumers»). Información Pre-contractual. Derecho de desistimiento. Otras normativas aplicables. Mecanismos Alternativos de Resolución de Conflictos: «ADRs» y «ODRs»[1] y otras recientes medidas de protección de consumidores en la Unión Europea (El «Nuevo Acuerdo para los Consumidores»). Mecanismos Alternativos de Resolución de Conflictos: «ADRs» y «ODRs». El «Nuevo Acuerdo para los Consumidores. II. Normativa de Protección de Datos y Privacidad en España y la Unión Europea. De la Declaración Universal de los Derechos Humanos al Reglamento Europeo de Protección de Datos. III. Normativa relativa a la Sociedad de Servicios de la Información. Cookies y Comunicaciones Comerciales.

1. Comúnmente se utilizan sus siglas y denominaciones en lengua inglesa; «ADR»: (*Alternative Dispute Resolutions*) y «ODR»: (*On line Disputes Resolutions*). De forma menos habitual se utilizan otras siglas correspondientes a denominaciones equivalentes o similares en lengua castellana; «RAL»: (*Resolución Alternativa de Litigios*) o «RAC»: (*Resolución Alternativa de Conflictos*).

Las Cookies. Concepto y finalidad. Implementación de las obligaciones establecidas en la normativa de Cookies. Tipología de Cookies. Comunicaciones Comerciales. IV. Breve referencia a la normativa bancaria y al estándar de seguridad «PCI-DSS». V. Derecho de la Competencia. Nuevas medidas sobre geobloqueo. NUEVAS NORMATIVAS RELEVANTES EN RUSIA Y CHINA. Rusia y el almacenamiento, tratamiento y localización de datos. Nueva regulación sobre ciberseguridad en China (La «CSL»). ¿«NUEVOS»? RETOS PLANTEADOS. BIBLIOGRAFÍA

Resumen

El presente trabajo pretende ser un instrumento sencillo y práctico que sirva de herramienta útil de consulta a profesionales (abogados o no) o empresarios que, de alguna manera, están relacionados con la explotación de negocios en línea. Una «guía» sencilla de las normativas más habituales que aplican al Comercio Electrónico que sirva como instrumento de utilidad para aquellas personas que no están familiarizadas con el marco legal o quieren acercarse un poco más a dicho marco y conocer su impacto en la práctica, operativa y día a día de las empresas. En consecuencia, el enfoque de este trabajo es, sin perder el necesario rigor jurídico, también, en parte, de carácter práctico. Huyendo de grandes disquisiciones jurídicas y análisis en profundidad, la presente obra se centra en las características esenciales y problemáticas legales (y, en algunos casos, de otra «naturaleza») más comunes y habituales. Cuestiones a analizar tanto en el momento del lanzamiento del negocio como durante toda la vida del mismo.

Palabras clave

Comercio Electrónico.

1. INTRODUCCIÓN

Resulta conveniente y necesario que el lector, antes de que acometa la lectura de este trabajo, conozca y entienda cómo ha sido el proceso de elaboración del mismo y su finalidad última. El origen de este documento se encuentra o, mejor dicho, se gesta poco a poco, en múltiples conversaciones, más o menos formales, con varios profesionales y de diferente perfil que ejercen su desempeño profesional en el mundo de las tecnologías. Además de abogados, nos referimos a profesionales del mundo del marketing digital y las redes sociales, de la protección de la privacidad y los datos de carácter personal, informáticos y desarrolladores, emprendedores, controllers y un largo etc. Con ellos se comparte, además del día a día profesional, comunes problemáticas y retos necesitados de soluciones jurídicas no siempre «disponibles» o no del todo acordes a la realidad que deben regular.

Habitualmente decimos que «el Derecho va por detrás de la realidad» pero, en este ámbito, esa afirmación tiene si cabe un mayor sentido. En todo lo relativo al mundo de las nuevas tecnologías en general y del Comercio Electrónico en particular, el Derecho tiene una especial y lógica dificultad para seguir a la realidad a la que se

enfrenta. Una realidad cambiante, inmediata, viral, sin una ubicación concreta pero a la vez global. Además de lo aprendido durante el ejercicio profesional, lo que aquí se contiene también nace y bebe de múltiples ponencias recibidas e impartidas y en las que se han intercambiado impresiones, dudas e inquietudes y no solo técnico-legales sino también relativas a prácticas, procedimientos y operativas. Los distintos retos que se nos presentan ante la mal llamada «era de la transformación digital». Y decimos mal llamada «era de la transformación digital» porque, a día de hoy, este término se muestra trasnochado y caduco. La tecnología ya es parte de todo y de todos y desde su raíz. No descubrimos nada nuevo ni a nadie al afirmar con rotundidad que, desde hace ya mucho tiempo, no hay nada en transformación sino que estamos ante una era plenamente digital y de «digitalización exponencial».

La idea es y, según se quiera ver, tan ambiciosa o simplista, la de elaborar un instrumento sencillo y práctico de trabajo que sirva de herramienta útil de consulta a profesionales (abogados o no) o empresarios que, de alguna manera, están relacionados con la explotación de negocios en línea. Una «guía» sencilla de las normativas más habituales que aplican al Comercio Electrónico que sirva como instrumento de utilidad para aquellas personas que no están familiarizadas con el marco legal o quieren acercarse un poco más a dicho marco y conocer su impacto en la práctica, operativa y día a día de las empresas. En consecuencia, el enfoque de este trabajo es, sin perder el necesario rigor jurídico, también, en parte, de carácter práctico. Huyendo de grandes disquisiciones jurídicas y análisis en profundidad, la presente obra se centra en las características esenciales y problemáticas legales (y, en algunos casos, de otra «naturaleza») más comunes y habituales. Cuestiones a analizar tanto en el momento del lanzamiento del negocio como durante toda la vida del mismo.

Es importante aclarar que el presente trabajo trata sobre Comercio Electrónico y no sobre Internet o la presencia en Internet. El escenario de base es del asesoramiento respecto de sitios web propios, de venta de productos (principalmente) y servicios (en menor medida) y en canal negocio-cliente/consumidor[2]. No obstante, pueden aparecer a lo largo del documento referencias a otros modelos o canales, tales como, venta a través de plataformas de terceros, cuestiones que tengan que ver con el canal negocio-negocio[3] o relativas a otro tipo de sitios web (redes sociales, webs divulgativas, etc.) pero, como se indica será a modo de mera referencia puntual y de ser necesaria en el contexto y con el enfoque descrito.

En términos sencillos, se podría definir el Comercio Electrónico como la realización de transacciones comerciales en un entorno electrónico y/o tecnológico y consistente principalmente en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet[4]. También es necesario

2. Conocido por sus siglas y denominación en lengua inglesa. B2C: «*Business to Consumer*».

3. Conocido por sus siglas y denominación en lengua inglesa. B2B: «*Business to Business*».

4. Así, en el ámbito de la Unión Europea (Comunicación de la Comisión 18 de abril de 1997, pero aún actual) se ha descrito el Comercio Electrónico como la actividad económica que, basada en el tratamiento electrónico y la transmisión de datos (ya sea en formato texto, imagen o video) abarcan en realidad actividades múltiples y muy diversas que van desde el intercambio de bienes y servicios a la entrega en línea de información digital, pasando por la transferencia electrónica de fondos, la actividad bursátil, la contratación pública. Dichas actividades pueden clasificarse en dos categorías: (i) el comercio electrónico indirecto, esto es, el pedido electrónico de bienes tangibles cuya entrega debe realizarse físicamente, por lo que depende de factores externos tales como la eficacia del sistema de transporte y de los servicios de correos y (ii) el comercio indirecto, es decir, el pedido en línea, el pago y la entrega de bienes y servicios intangibles tales como los programas informáticos o productos de esparcimiento.

aclarar que no se trata de un trabajo sobre Comercio Electrónico entendido en sentido amplio sino, muy concretamente, sobre el trabajo de asesorar legalmente en materia de Comercio Electrónico e identificar las cuestiones básicas y esenciales en relación con ese asesoramiento.

Desde un punto de vista del análisis normativo, nos centraremos principalmente en el ámbito nacional y el entorno de la Unión Europea. Y ello porque creemos que este marco legal es el que más directa y habitualmente «afecta» a la mayoría de los sitios webs operados desde España. Sin embargo, por la relevancia de los mercados en cuestión y el interés lógico que estos mercados tienen, haremos una mención final a ciertos cambios normativos muy relevantes aprobados recientemente en Rusia y China. Como se verá, las nuevas leyes aprobadas, que más adelante trataremos, impactan directamente en los costes a afrontar y la estructura tecnológica y operativa a montar para todos aquellos que quieran vender en línea en estos dos países. Como referencia final y abierta, señalaremos algunos de los nuevos retos a los que nos enfrentamos y resultado lógico e inevitable de la evolución tecnológica.

2. PROBLEMÁTICAS Y PARTICULARIDADES DEL ASESORAMIENTO LEGAL EN MATERIA DE COMERCIO ELECTRÓNICO

Las problemáticas a las que un profesional se enfrenta cuando asesora en materia de Comercio Electrónico derivan de varias circunstancias que confluyen a la vez y que, entre otras muchas, son las que más adelante señalamos.

I. Por el ámbito material

En primer lugar, hay que tener en cuenta que el Comercio Electrónico como tal, es una actividad económica en sí misma y que, por tanto, engloba la aplicación de diferentes normativas. Esto es, todas las que resultan aplicables a cualquier actividad económica así como las específicas del Comercio Electrónico y la actividad en cuestión. Así, y a modo de mera indicación y como listado «abierto», las normativas a revisar podría ser las relativas a:

- Normativa reguladora del Comercio Electrónico, Venta a Distancia, Consumo y Comercio[5].
- Normativa de Protección de Datos y Privacidad.
- Normativa de Sociedad de la Información o Internet, Digital Marketing y Comunicaciones Comerciales.
- Normativa Bancaria Regulatoria así como estándares de seguridad en materia de medios de pago (por ejemplo, *PCI-DSS*).
- Derecho de la Competencia.
- Normativa de Telecomunicaciones.
- Normativa sobre Blanqueo de Capitales.

5. En el ámbito nacional, además y como se verá a continuación, tanto con carácter estatal como autonómica.

- Normativa penal; suplantación de identidad y fraude.
- Normativa de Etiquetado (doble prisma: desde el punto de vista del propio producto así como respecto de la presentación del mismo en el sitio web).
- Ciberseguridad.
- Normativa sobre Aduanas.
- Fiscalidad.
- Cuestiones relativas a Propiedad Intelectual.
- Derecho laboral y Prevención de Riesgos laborales.
- Cualquier otra que resultara de aplicación según las posibles particularidades de los países en lo que el sitio web esté presente.
- Normativa sectorial aplicable a los productos o servicios ofrecidos.
- ¿Otras....? las materias que en este trabajo se relacionan o mencionan son, en opinión del autor, las más significativas y recurrentes pero, no solo se trata de una valoración subjetiva sino que «*ni son todas las que están ni están todas las que son*....».

II. Por el ámbito geográfico

Además de lo anterior, nos enfrentamos también al hecho de que la globalidad e internacionalidad propia del Comercio Electrónico implica necesariamente la aplicación de las normativas de las diferentes jurisdicciones implicadas. Especialmente aquellas normativas de carácter imperativo. De entre las múltiples ventajas que a los comerciantes puede otorgar la venta en línea frente a otros canales como, el establecimiento abierto al público, una muy relevante es la posibilidad de ofrecer a la venta los productos en varios países simultáneamente. La consecuencia de esto es que al Comercio Electrónico que se lleve a cabo no solo en España sino en otros países resultarán de aplicación todas las normas y de todas las áreas en las que el sitio web esté presente. Esto es indudable además respecto de aquellas que revistan carácter imperativo.

III. Por las particularidades del canal

Otras particularidades muy relevantes a tener en cuenta resultan de la propia naturaleza de Internet. Nos referimos principalmente y como ya anticipábamos a: la viralidad, visibilidad, globalidad e inmediatez. Cualquier tipo de error en el asesoramiento o cualquier tipo de infracción o incumplimiento (incluso el mero rumor de incumplimiento, cierto o no) puede tener un efecto negativo difícilmente ponderable y evitable apriorísticamente. Las posibles consecuencias legales y fácticas de cualquier incumplimiento (o, simplemente, el rumor que de que se ha producido el mismo) pueden ser globales, internacionales, altamente visibles, inmediatas y con un impacto reputacional y legal difícilmente ponderable según cuál sea el caso. La repercusión puede tener lugar asimismo en distintos niveles; no solo a nivel de usuarios, autoridades o tribunales sin también en otros de perfil más mediático, tales como, redes sociales, foros de discusión o blogs.

IV. Por la naturaleza de las cuestiones objeto de análisis

Si se pretende contar con un análisis detallado y adecuado será necesario analizar, en nuestra opinión y adicionalmente a la normativa aplicable, al menos, las siguientes cuestiones: (i) procesos de compra completos y en su sentido más amplio, incluyendo, por tanto, pagos y devoluciones (ii) cuestiones legales que afecten a cuestiones técnicas o de Sistemas (localización de servidores, requisitos de accesibilidad para discapacitados, etc.), (iii) estándares internacionales y nacionales, vinculantes o de «soft law» que, en su caso, afecten o puedan afectar a la presentación del producto, las funcionalidades y/o el «look and feel» o «front» (e.g, labelling, accesibilidad, buen gobierno y la subsiguiente obligación de incluir, por ejemplo, links a autoridades o asociaciones, ubicaciones concretas de funcionalidades o contenidos, –footer, pop up, link directo, etc–), (iv) Términos y Condiciones de las webs, redes sociales y/o plataformas de terceros donde esté presente directa o indirectamente la web en cuestión, así como, (v) la obtención de los necesarios consentimientos en cuestiones tales como cookies, políticas de privacidad, comunicaciones comerciales o retargeting.

Hay que tener en cuenta que como resultado de que, como hemos indicado, nos encontramos ante transacciones comerciales habrá que revisar con mucha cautela y detalle los diferentes contratos y relaciones jurídicas con terceros que dicha actividad vaya a implicar. Entre otros muchos, por su particularidad, destacamos los contratos con proveedores de medios de pago y entidades bancarias o financieras. Y no solo en relación a los medios de pago tradicionales como los relativos a tarjetas de crédito, transferencias o pagos contra reembolso o en metálico, sino también todo lo relativo a los nuevos medios de pago que surgen en el contexto del Comercio Electrónico; pasarelas de pago, bitcoins, fintechs y/o modos de pago «wallet», por ejemplo.

Muy relevante es también la regulación contractual relativa al marketing digital; contratos de afiliación, redes sociales, agencias de publicidad y comunicación, bloggers, analytics, etc. así como la ligada a la propia operativa de un sitio web (logística, almacén y transporte).

V. Por el contenido y formato del análisis. El «Entregable»

Ligado a lo señalado en el apartado anterior es que el contenido del análisis y la forma en que este se presenta, sin dejar de ser legal, suele ser distinto al habitual. La práctica ha puesto de manifiesto que el asesoramiento en materia de Comercio Electrónico no puede quedarse simplemente en la elaboración de análisis e informes jurídicos sino que debe contar con elementos adicionales de apoyo y valoración a las diferentes áreas de negocio como sistemas, marketing, logística, etc. Pongamos algunos ejemplos de lo que nos referimos.

- Descripción del marco normativo aplicable y la práctica jurisprudencial, inspectora y sancionadora.
- Relación de los posibles incumplimientos y/o cuestiones que pudieran necesitar actuaciones de adecuación.
- Análisis de riesgos por categorías y según la práctica del país. Es muy complicado, sino casi imposible, cumplir con todas las normativas y en todos los países, por lo tanto, resulta necesario una priorización basada en criterios sólidos y contrastados. Dichos criterios a valorar podrían ser los siguientes:

- Criterios de interpretación, precedentes judiciales, sentencias, etc., de autoridades y tribunales.
- Mayor o menor severidad en el importe de las sanciones así como naturaleza de las mismas (pecuniarias, reputacionales, etc.).
- Precedentes de inspecciones y sanciones, distinguiendo sectores y cuestiones más inspeccionadas.
- Procedimiento (apercibimientos, subsanaciones, sanción directa, etc.).

• Benchmarking y «best pactices» recomendadas por las diversas instituciones, asociaciones u organismos reguladores.

• Impacto en el sitio web y sus contenidos en el sentido de cómo se presentan dichos contenidos.

3. NORMATIVAS MÁS RELEVANTES EN RELACIÓN CON EL COMERCIO ELECTRÓNICO

Veamos ahora, con algo más de detalle, las normativas más relevantes y habituales que hay que tener en cuenta cuando se asesora en materia de Comercio Electrónico. Este análisis será necesario no solo en el momento del lanzamiento de un sitio web sino de forma recurrente durante toda la vida del mismo. Aclarar que de todas las que hemos señalado anteriormente y, dejando clara constancia de que todas son igual de relevantes, nos centraremos en analizar solo algunas de ellas y solo respecto de algunas cuestiones que entendemos más recurrentes, actuales y con mayor impacto en las empresas. Se trata, por tanto, de una selección absolutamente subjetiva, basada en la experiencia y que responde únicamente a una priorización de criterio personal a los efectos de este trabajo.

I. Normativa de Consumo y Comercio con especial consideración del derecho de desistimiento y la información Pre-contractual. Los Mecanismos Alternativos de Resolución de Conflictos (ADR/ODR) y otras medidas recientes de protección a los consumidores en el ámbito de la Unión Europea («*New Deal for Consumers*»)

Es posiblemente la primera y más importante normativa que hay que analizar cuando se asesora en Comercio Electrónico. Se da la especial circunstancia de que, por un lado, van a confluir la normativa nacional y la de los países donde el sitio web esté operando[6]; por otro, que, en España, (y en algún otro país de nuestro entorno ocurre algo similar[7]) y como resultado de la organización territorial del Estado, habrá que dar cumplimiento no solo a la normativa estatal sino también a la autonómica.

Centrémonos en España y, en particular, en la normativa estatal. En el ámbito nacional, la principal norma que resulta de aplicación al Comercio Electrónico sería

6. En materia de consumo, esta normativa, además, suele ser de carácter imperativo en la mayoría de los países y respecto de la mayoría de sus articulados en esta cuestión.

7. Por ejemplo, en Italia, que aplica el Decreto Legislativo no. 114/1998 regulador del Sector del Comercio pero también las Leyes Regionales. Otro caso significativo es Suiza donde el consumo se rige por el artículo 97 de la Constitución federal, la Ley Federal de Información al Consumidor y, según los casos, por los reglamentos de los diferentes Cantones.

el 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 (en adelante, LGCU). La LGCU viene a regular aspectos esenciales como, por ejemplo, los derechos básicos de consumidores y usuarios y la protección de sus legítimos intereses económicos, contratos y garantías, derechos de desistimiento, cláusulas abusivas, obligaciones previas de información o las garantías y servicios post-venta. Es importante señalar que la LGCU contiene, en su Título III, una regulación específica relativa los Contratos celebrados a distancia y contratos celebrados fuera del establecimiento mercantil. En relación con esta regulación, merecen especial mención las disposiciones relativas al derecho de desistimiento y la información pre-contractual que esbozamos muy brevemente.

a. Información Pre-contractual

Conforme al artículo 97 de la LGCU el empresario debe facilitar con anterioridad a cualquier transacción y de forma clara y comprensible, entre otra, la siguiente información:

- Las características principales de los bienes o servicios.
- La identidad del empresario, incluido su nombre comercial.
- La dirección completa del establecimiento del empresario y el número de teléfono, número de fax y dirección de correo electrónico del mismo, cuando proceda, con objeto de que el consumidor y usuario pueda ponerse en contacto y comunicarse con él de forma rápida y eficaz, así como, cuando proceda, la dirección completa y la identidad del empresario por cuya cuenta actúa.
- El precio total de los bienes o servicios, incluidos los impuestos y tasas.
- El coste de la utilización de la técnica de comunicación a distancia para la celebración del contrato, en caso de que dicho coste se calcule sobre una base diferente de la tarifa básica.
- Los procedimientos de pago, entrega y ejecución, la fecha en que el empresario se compromete a entregar los bienes o a ejecutar la prestación de los servicios, así como, cuando proceda, el sistema de tratamiento de las reclamaciones del empresario.
- La lengua o lenguas en las que podrá formalizarse el contrato, cuando ésta no sea la lengua en la que se le ha ofrecido la información previa a la contratación.
- Cuando exista un derecho de desistimiento, las condiciones, el plazo y los procedimientos para ejercer ese derecho, así como el modelo de formulario de desistimiento.
- Cuando proceda, la indicación de que el consumidor y usuario tendrá que asumir el coste de la devolución de los bienes en caso de desistimiento y, para los contratos a distancia, cuando los bienes, por su naturaleza, no puedan devolverse normalmente por correo, el coste de la devolución de los mismos.
- Un recordatorio de la existencia de una garantía legal de conformidad para los bienes.

- Cuando proceda, la existencia de asistencia posventa al consumidor y usuario, servicios posventa y garantías comerciales, así como sus condiciones.
- La existencia de códigos de conducta pertinentes y la forma de conseguir ejemplares de los mismos, en su caso. A tal efecto, se entiende por código de conducta el acuerdo o conjunto de normas no impuestas por disposiciones.
- La duración del contrato, cuando proceda, o, si el contrato es de duración indeterminada o se prolonga de forma automática, las condiciones de resolución.
- Cuando proceda, la duración mínima de las obligaciones del consumidor y usuario derivadas del contrato.
- Cuando proceda, la existencia y las condiciones de los depósitos u otras garantías financieras que el consumidor y usuario tenga que pagar o aportar a solicitud del empresario.
- Cuando proceda, la funcionalidad de los contenidos digitales, incluidas las medidas técnicas de protección aplicables.
- Cuando proceda, toda interoperabilidad relevante del contenido digital con los aparatos y programas conocidos por el empresario o que quepa esperar razonablemente que éste pueda conocer.
- Cuando proceda, la posibilidad de recurrir a un mecanismo extrajudicial de reclamación y resarcimiento al que esté sujeto el empresario y los métodos para tener acceso al mismo.

b. Derecho de desistimiento

Se reconoce al consumidor y usuario el derecho a desistir del contrato durante un periodo de 14 días naturales sin indicar el motivo y sin incurrir en ningún coste[8]. El empresario reembolsará todo pago recibido del consumidor y usuario, incluidos, en su caso, los costes de entrega, sin demoras indebidas y, en cualquier caso, antes de que hayan transcurrido 14 días naturales desde la fecha en que haya sido informado de la decisión de desistimiento del contrato del consumidor y usuario.

El empresario deberá efectuar el reembolso utilizando el mismo medio de pago empleado por el consumidor para la transacción inicial, a no ser que el consumidor haya dispuesto expresamente lo contrario y, siempre y cuando, el consumidor no incurra en ningún gasto como consecuencia del reembolso. Serán nulas de pleno derecho las cláusulas que impongan al consumidor y usuario una penalización por el ejercicio de su derecho de desistimiento o la renuncia al mismo.

c. Otras normativas aplicables

A modo de simple referencia, mencionamos otras dos normativas que consideramos importante tener en cuenta en caso de resultar de aplicación. Nos referimos a la

8. A salvo de las excepciones contempladas en los artículos 107 y 108 y relativos a la selección por el usuario, una modalidad de entrega diferente a la modalidad menos costosa de entrega ordinaria o los costes directos de devolución de los bienes, salvo si el empresario ha aceptado asumirlos o no le ha informado de que le corresponde asumir esos costes.

Ley 7/1996 de Ordenación del Comercio Minorista y a la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación.

En el contexto de la venta minorista, la Ley de Ordenación del Comercio Minorista establece las condiciones especiales que se aplican a las ventas realizadas «a distancia», es decir, las ventas celebradas sin la presencia física simultánea del comprador y del vendedor. Ello siempre que su oferta y aceptación se realicen de forma exclusiva a través de una técnica cualquiera de comunicación a distancia y dentro de un sistema de contratación a distancia organizado por el vendedor. Debemos aclarar que a los efectos de dicha Ley, se entenderá por comercio minorista la actividad desarrollada profesionalmente con ánimo de lucro consistente en ofertar la venta de cualquier clase de artículos a los destinatarios finales de los mismos, utilizando o no un establecimiento.

Por su parte, la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación, es la referencia a los efectos de la distinción entre lo que son cláusulas abusivas de lo que son condiciones generales de la contratación. Esta cuestión es básica cuando se preparen y redacten los Términos y Condiciones de Uso y/o Compra o documentos similares así como en la definición de los aspectos operativos del sitio web en cuestión.

d. Mecanismos Alternativos de Resolución de Conflictos: «ADRs» y «ODRs»[9] y otras recientes medidas de protección de consumidores en la Unión Europea («El Nuevo Acuerdo para los Consumidores»)[10]

i Mecanismos Alternativos de Resolución de Conflictos: «ADRs» y «ODRs»

Tal y como puso de manifiesto la Comisión Europea en el pasado[11], garantizar el acceso de los consumidores a la justicia, no solo en tribunales ordinarios o especializados sino a través de otras instancias o mecanismos y de diversa naturaleza como la mediación, la conciliación y el arbitraje, era una cuestión esencial para la consecución de un mercado único.

Como resultado de lo anterior y con el fin de alcanzar la finalidad indicada, se aprobarían, en el año 2013, simultánea y conjuntamente, la Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo (en adelante, la Directiva 2013/11/UE) y el Reglamento (UE) n.º 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo (en adelante, el Reglamento 524/2013). En España, la Ley 7/2017, de 2 de noviembre traspuso al ordenamiento jurídico español la Directiva 2013/11/UE.

9. Comúnmente se utilizan sus siglas y denominaciones en lengua inglesa; «ADR»: (*Alternative Dispute Resolutions*) y «ODR»: (*On line Disputes Resolutions*). De forma menos habitual se utilizan otras siglas correspondientes a denominaciones equivalentes o similares en lengua castellana; «RAL»: (*Resolución Alternativa de Litigios*) o «RAC»: (*Resolución Alternativa de Conflictos*).

10. Traducción libre y no oficial al castellano de su denominación en lengua inglesa: «*New Deal for Consumer*».

11. Nos referimos, por ejemplo, a las comunicaciones remitidas al Consejo Europeo en 1985 y 1987, la Resolución del Consejo de la CEE de 25 de junio de 1987, sobre el acceso de los consumidores a la justicia y sobre todo el Libro Verde de 16 de noviembre de 1993 sobre el acceso de los consumidores a la justicia y solución de litigios en materia de consumo en el mercado único.

Las regulaciones indicadas anteriormente tratan de asegurar, a través de un alto nivel de protección del consumidor y tanto respecto del consumo en general como del consumo en línea, el buen funcionamiento del mercado interior. Se pretende garantizar que los consumidores puedan, si así lo desean, presentar reclamaciones contra los comerciantes ante entidades que ofrezcan procedimientos de resolución alternativa de litigios y, de esta forma, establecer un sistema de procedimientos que sean independientes, imparciales, transparentes, efectivos, rápidos y justos. En concreto, el Reglamento 524/2013 y con el ánimo indicado, crea una Plataforma de resolución de litigios en línea (en adelante, la «Plataforma») que constituye una ventanilla única para los consumidores y comerciantes que deseen resolver extrajudicialmente los litigios incluidos en el ámbito de aplicación del presente Reglamento. Se trata de un sitio de internet interactivo al que se podrá acceder de forma electrónica y gratuita en todas las lenguas oficiales de las instituciones de la Unión Europea. Volveremos más adelante sobre esta cuestión centrándonos ahora en el ámbito de aplicación.

En cuanto al ámbito geográfico, téngase en cuenta que estos procedimientos de resolución extrajudicial pueden aplicarse tanto respecto de litigios nacionales como transfronterizos. Su ámbito material se circunscribe a las obligaciones contractuales derivadas de contratos de compraventa o de prestación de servicios (también los celebrados en línea, de ser caso). En cuanto a los sujetos legitimados, será necesario que se refieran a conflictos o litigios entre un comerciante establecido en la Unión Europea y un consumidor residente en la Unión Europea.

Como anticipábamos, el Reglamento 524/2013 constituyó una Plataforma con las siguientes funciones:

- Facilitar un formulario electrónico de reclamación a ser completado por la parte reclamante.
- Informar de la reclamación a la parte reclamada.
- Determinar la entidad o entidades de resolución alternativa competentes y transmitir la reclamación a la entidad de resolución alternativa que las partes hayan acordado utilizar.
- Ofrecer gratuitamente un sistema electrónico de tramitación de asuntos que permita a las partes y a la entidad de resolución alternativa tramitar en línea el procedimiento de resolución de litigios a través de la Plataforma.
- Proporcionar a las partes y a la entidad de resolución alternativa la traducción de la información que sea necesaria para la resolución del litigio y que se intercambie a través de la Plataforma.
- Facilitar un formulario electrónico del que se servirán las entidades de resolución alternativa para transmitir la información principal relativa al litigio.
- Proporcionar un sistema de comentarios que permita a las partes expresar su opinión sobre el funcionamiento de la Plataforma y sobre la entidad de resolución alternativa que haya conocido de su litigio.
- Poner a disposición pública lo siguiente:
  - o Información general sobre la resolución alternativa de litigios como forma de resolución extrajudicial de litigios.

- Información sobre las entidades de resolución alternativa incluidas en la lista con arreglo al artículo 20, apartado 2, de la Directiva 2013/11/UE que sean competentes para conocer de los litigios incluidos en el ámbito de aplicación del Reglamento 524/2013.
- Un manual en línea sobre el modo de presentar reclamaciones a través de la Plataforma.
- Información, incluidos los datos de contacto, acerca de los puntos de contacto de resolución de litigios en línea designados por los Estados miembros.
- Datos estadísticos del resultado de los litigios sometidos a entidades de resolución alternativa a través de la Plataforma.

Hagamos un resumen de las fases del procedimiento que ha establecido la Unión Europea y centrándonos en el correspondiente a la resolución de litigios en línea. Inicialmente, el consumidor completa el formulario de reclamación en línea y lo envía desde la propia Plataforma[12]. Una vez presentado el formulario, se da traslado de la reclamación al vendedor quien propone al consumidor una entidad de resolución alternativa del conflicto.

En caso de que consumidor y vendedor se pongan de acuerdo en la entidad de mediación que va a resolver su conflicto, la Plataforma se lo remite a dicha entidad que dilucidará sobre el asunto en cuestión en base al principio de equidad.

La entidad de mediación se ocupa del caso por vía electrónica y propone una solución en el plazo de 90 días. La decisión que adopte la entidad de resolución alternativa con respecto al litigio que ante ella se tramite puede presentar dos caracteres distintos: proponer una solución que facilite un acuerdo amistoso o imponer a las partes la solución a la que se haya llegado al finalizar el procedimiento. En relación al precio, el acceso será gratuito salvo que en el devenir del procedimiento se devenguen costes que, en todo caso, serán asequibles para las partes.

Igualmente y por la visibilidad que a estos procedimientos se pretende otorgar, es importante mencionar la obligación de información contenida en el artículo 14 del Reglamento 524/2013. Según esta disposición, los comerciantes establecidos en la Unión que celebren contratos de compraventa o de prestación de servicios en línea y los mercados en línea establecidos en la Unión ofrecerán en sus sitios de Internet un enlace electrónico a la Plataforma de resolución de litigios en línea. Dicho enlace será de fácil acceso para los consumidores[13].

ii. El «Nuevo Acuerdo para los Consumidores»

No querríamos finalizar el presente epígrafe sin dejar de hacer mención a un importante paquete de medidas llevadas a cabo recientemente en el seno de la Unión Europea. Nos referimos a las propuestas e iniciativas conocidas como el «Nuevo

12. Téngase en cuenta que, incluso en el caso de que estemos fuera del ámbito de los litigios en línea, estas opciones vinculadas a dicho entorno siguen siendo potenciadas por la normativa europea. Así, la Directiva 2013/11/UE establece que los Estados Miembros garantizarán que las entidades de resolución alternativa mantengan un sitio de internet actualizado que facilite a las partes un acceso sencillo a la información relativa al procedimiento de resolución alternativa y permita además a los consumidores presentar en línea una reclamación junto con los documentos justificativos necesarios.

13. El enlace es el siguiente: *http://ec.europa.eu/consumers/odr/*.

Acuerdo para los Consumidores» y adoptadas por la Comisión Europea el 11 de abril de 2018. El «Nuevo Acuerdo para los Consumidores» comprende dos Directivas y una Comunicación y que están dirigidas principalmente a reforzar los derechos de los Consumidores y regular posibles compensaciones individuales a los mismos, analizar determinadas actuaciones y prácticas comerciales irregulares y «modernizar» la legislación de la Unión Europea a la luz de la evolución del mercado y especialmente en materia digital. Adicionalmente, estas iniciativas incluyen entre sus finalidades últimas y principales la de potenciar las acciones colectivas. También, pero en menor medida, están presentes algunas medidas de protección a los comerciantes. Entre ellas, destacar la relativa a la no obligatoriedad de reembolso antes de recibir los productos objeto de devolución o la de no tener que aceptar la devolución de productos usados (en exceso de una prueba) así como la consistente en dotar de una mayor flexibilidad a los canales en los que los comerciantes se comunican con los consumidores (formularios web, chats, etc.).

En línea con lo señalado, destacamos algunas de las medidas concretas adoptadas. Se mejora la transparencia en las plataformas market places y los resultados de las búsquedas. Se entiende que se tiene que saber con certeza a quién se está comprando y, en consecuencia, se impone a las plataformas la obligación de informar si se está comprando a un comerciante o a un particular. En cuanto a las búsquedas, el usuario deberá ser informado de si un resultado es gratuito o no y cuáles son los principales parámetros que determinan el ránking de resultados.

Se podrán analizar las prácticas comerciales engañosas relativas a la posible comercialización de productos como si fueran idénticos cuando su composición o sus características son en realidad significativamente diferentes (calidad dual de los productos de consumo).

En materia de acciones colectivas, se reconoce a las entidades cualificadas[14] la posibilidad de ejercitar dichas acciones en determinados supuestos. En nuestra opinión, la Unión Europea, si bien trata de ampliar el elenco de las posibles responsabilidades (y correspondientes compensaciones) ante grupos afectados por un mismo hecho, a la vez, establece limitaciones que hace que no estemos ante un esquema puro de acción a modo de «Acciones de Clase»[15] de Estados Unidos sino un tipo de reclamación más acotada tanto subjetiva como materialmente. Así, las posibles demandas podrán versar sobre la violación de múltiples derechos u obligaciones y en sectores de lo más variado, tales como, entre otros; medioambiente, comunicaciones, entorno financiero, aseguradoras. No obstante, las entidades demandantes deberán informar en el contexto de estas acciones sobre su capacidad financiera y el origen de los fondos que soportan la demanda en cuestión.

Las acciones colectivas podrán incluir desde medidas provisionales a definitivas para detener o prohibir determinada práctica si pueden suponer o suponen infraccio-

14. La cualificación o no como «entidad cualificada» será determinada por los Estados miembros y, para ello, deberán cumplir una serie de criterios para asegurar, principalmente, que se tratan de organizaciones sin ánimo de lucro.

15. Las conocidas como «*Class Actions*» y que se regulan en la ley procesal americana. En concreto, en la *Federal Rule no. 23 of Civil Procedure*. En ellas, a diferencia de lo indicado en el seno de la Unión Europea, la legitimación para defender los derechos individuales del colectivo reside en uno o varios representantes del propio grupo, liderados por el abogado o abogados asesores y en relación con diferentes tipos de causas que sean de común interés al mencionado colectivo.

nes normativas. Asimismo, la norma protege y promueve la resolución de la disputa a través de un acuerdo extrajudicial.

II. Normativa de Protección de Datos y Privacidad en España y la Unión Europea. De la Declaración Universal de los Derechos Humanos al Reglamento Europeo de Protección de Datos

Muchos autores (y compartimos dicha opinión) han situado la génesis de la protección de datos de carácter personal en la Declaración Universal de los Derechos Humanos de 1948 y, en concreto, en su consagración del principio de no injerencia en la vida privada y familiar. Partiendo como hito de partida el hecho mencionado, pasemos ahora a analizar brevemente la evolución de esta normativa en el ámbito nacional y europeo en los últimos años y hasta el reciente Reglamento de Protección de Datos.

En relación con la regulación de estas cuestiones en el ámbito nacional, entendemos que debemos situar en el contexto de la transición y, en concreto, de la Constitución de 6 de diciembre de 1978. Así, el art. 18 de la Constitución Española de 1978[16], ya establecía con rango de derechos fundamentales el derecho al honor, a la intimidad personal y familiar, a la propia imagen y al secreto de las comunicaciones. Todo ello, además, estableciendo expresamente que la ley limitaría el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Consecuencia del contenido del mencionado artículo en su apartado cuarto fue la aprobación, entre otras, de sendas leyes Orgánicas separadas por un período de 10 años. Por un lado, la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen y, por otro, de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Esta última tenía por objeto limitar el uso de la informática y otras técnicas así como los medios de tratamiento automatizado de los datos de carácter personal para garantizar los derechos fundamentales señalados. La norma, vigente hasta el 14 de enero de 2000 fue objeto de desarrollo mediante el Real Decreto 1332/1994, de 20 de junio pero, como veremos después, muy pronto superada.

También en línea como lo establecido en la Constitución Española, la Ley Orgánica 10/1995, de 23 de noviembre, por la que se aprobaba el Código Penal actualmente en vigor, vino a elevar al ámbito del Derecho Penal la tutela de estos derechos. En particular, el art. 197.2 del Código Penal estableció, como tipo punible, la actuación de aquel que «sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».

Los siguientes referentes normativos relevantes y prácticamente coetáneos a la aprobación del CP se encuentran en al ámbito comunitario y suponen el verdadero hito de referencia para el marco normativo vigente en nuestro ordenamiento. Nos

16. El art. 18.4 de la CE reza «*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*».

referimos, por supuesto, a la Directiva 95/46/CE y, en menor medida, al Convenio Nº 108 del Consejo de Europa, de 28 de Enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. El Convenio 108 estableció como «deseable» la ampliación de la protección de los derechos y de las libertades fundamentales al respeto de la vida privada pero reconociendo, al mismo tiempo, el necesario respeto al compromiso en favor de la libertad de información y el flujo de información entre los pueblos. Será con la promulgación de la Directiva 95/46/CE cuando los Estados Miembros asuman ya un firme compromiso de garantizar el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Para llevar esto a efecto se establecieron los principios que debían regir los pilares de la regulación de la protección de datos de carácter personal; a saber, la definición y delimitación de los conceptos fundamentales, los principios para la licitud del tratamiento y el establecimiento de los derechos básicos de protección del «interesado».

Como consecuencia de los principios constitucionales y de la necesidad de trasponer la normativa comunitaria anteriormente citada, con fecha 13 de diciembre de 1999, se aprobó la Ley Orgánica 15/1999, de Protección de datos de carácter personal (conocida comúnmente como la «LOPD»). La LOPD adaptó nuestro ordenamiento lo dispuesto por la Directiva 95/46/CE y derogó la hasta entonces vigente Ley de 1992[17].

Debemos destacar que, tras la aprobación de la LOPD, el Tribunal Constitucional rompe con el concepto que recogía en diversas sentencias anteriores sobre el derecho a la protección de datos como parte del derecho a la intimidad y privacidad, y en la Sentencia 292/2000, de 30 de noviembre de 2000, del Tribunal Constitucional, estableció expresamente la independencia del derecho fundamental a la protección de datos.

La LOPD, siguiendo en gran parte la sistemática y el contenido de la Directiva 95/46/CE, contempló, además de los aspectos de dicha norma anteriormente citados[18], los siguientes; el derecho de oposición como un nuevo derecho básico del interesado, la regulación de la transferencia internacional de datos y el establecimiento de los principios rectores de la naturaleza jurídica y funciones esenciales de la Agencia Española de Protección de Datos (en adelante, «AEPD»).

Será en el año 2007 cuando mediante el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD se asumiría la finalidad y el reto de hacer frente a los riesgos que, para los derechos de la personalidad y de las personas, suponían (y suponen) la recopilación y tratamiento de datos de carácter personal en ficheros, ya sean estos automatizados o no. El RD 1720/2007 estableció una regulación detallada y precisa sobre la atribución de los niveles de seguridad (básico, medio y alto) así como de las correspondientes medidas de seguridad requeridas para cada caso. A tal fin, su Título VIII contiene una descripción de medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad que garanticen la protección, confidencialidad, integridad y disponibilidad de los recursos. Y ello con independencia de que se trate

17. No así su normativa de desarrollo, esto es, el RD 1332/1994 que siguió vigente hasta la aprobación del RD 1720/2007.

18. Esto es, la definición y delimitación de los conceptos fundamentales, los principios para la licitud del tratamiento y el establecimiento de los derechos básicos de protección del «interesado».

de soportes automatizados (informatizados) como no automatizados (papel u otros soportes físicos). Igualmente y como resultado de las nuevas obligaciones contempladas, las empresas fueron requeridas a describir las medidas de índole técnica y organizativas adoptadas y reflejar las mismas en un Documento de Seguridad

Creemos que merece la pena mencionar, aunque sea a modo de simple referencia, otras normativas aprobadas en España y relevantes en estas materias. Entre otras muchas posibles, destacamos el Real Decreto 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la Agencia de Protección de Datos, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios y la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

La normativa mencionada, si bien sigue en vigor, ha sido significativamente superada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, «el Reglamento»). Esta regulación ha venido a derogar la Directiva 95/46/CE y despliega su pleno vigor y eficacia el 25 de mayo de 2018. A partir de la fecha mencionada es, por tanto, directamente aplicable en todos los Estados Miembros y sin necesidad de transposición. En términos muy generales podemos destacar las siguientes cuestiones introducidas por el Reglamento y que han venido a suponer una modificación sustancial y desde todos los ámbitos respecto de la normativa actual. Como consecuencia directa y práctica va a implicar numerosos cambios en las operativas, procesos y relaciones con terceros de las empresas.

Un primer aspecto a destacar del Reglamento es que puede resultar de aplicación incluso a empresas no establecidas en la Unión Europea cuando se efectúe una oferta de bienes o servicios destinada a ciudadanos de la Unión Europea.

Se establecen los principios de autoregulación y responsabilidad proactiva así como la obligación de las empresas de demostrar su compromiso con los derechos de los ciudadanos y el cumplimiento de sus obligaciones legales[19] como elementos vertebradores de la protección de derechos en la organización y procesos de las empresas. Al responsable del tratamiento corresponde, no solo la obligación de dar cumplimiento a todas las previsiones normativas en materia de protección de datos sino, además, el estar en disposición y en todo momento de acreditar dicho cumplimiento.

Veamos con algo más de detalle estos principios. El principio de responsabilidad proactiva establece la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar que el tratamiento es conforme con el Reglamento. Muy ligado a lo anterior y, como se indicó, el principio de accountability impone a las organizaciones la obligación, no solo de cumplir, sino de evidenciar en todo momento que se cumple. Los responsables deberán implementar medidas técnicas y organizativas apropiadas para asegurar y poder demostrar que el

19. Principio más conocido por su denominación en lengua inglesa: «*accountability*» y que será el que usaremos en adelante.

tratamiento de datos se realiza de acuerdo con el Reglamento. Que las mencionadas medidas sean las apropiadas, en cada caso, dependerá de la naturaleza, alcance, contexto y fines del tratamiento así como los riesgos de los derechos y las libertades de las personas en liza.

Es de esperar que los anteriores principios supongan en la práctica la proliferación de aquellas figuras que favorezcan o prueben dicho compromiso; nos referimos a los Códigos de Conducta y que, en palabras de la propia AEPD: «destacan como una herramienta útil para demostrar que responsables y encargados cumplen con los requisitos establecidos en el mismo».

El Reglamento también viene a endurecer y reforzar las obligaciones impuestas a las empresas en materia de información y consentimiento. En cuanto a la información: resultará obligatorio indicar la base jurídica o legitimación del tratamiento de datos personales o los plazos o criterios de conservación de la información. Sobre la base del principio de transparencia, la información proporcionada deberá ser fácil de entender y tener un lenguaje simple y claro.

En cuanto al consentimiento y como cambio muy relevante se elimina la posibilidad de obtener un «consentimiento tácito». Ahora será preceptivo recabar un consentimiento libre, inequívoco e informado.

Asimismo, el Reglamento impone a las empresas que sufran una violación de seguridad la obligación de denunciar las mismas en un plazo de 72 horas. Igualmente y, en determinados casos, comunicar dicha violación de seguridad a usuarios, clientes o empresas afectada.

El elenco de medidas y obligaciones más significativas no termina en las anteriores sino que debemos mencionar algunas otras igualmente relevantes. Estas obligaciones también resultan, directa o indirectamente, del principio de responsabilidad activa y conllevan un enorme impacto en la organización, sistemas, procedimientos y operativas de las compañías. El Reglamento viene a establecer como nuevas obligaciones esenciales las de, en su caso, llevar a cabo un análisis de riesgos y un registro de actividades de tratamiento así como a consagrar los principios de protección de datos «desde el diseño» y «por defecto» y la obligación de nombrar un Delegado de Protección de Datos (conocido comúnmente como «DPO»)[20]. Comentemos, a continuación, sobre estas tres últimas cuestiones.

La protección de datos «desde el diseño» implicará la aplicación de las garantías de protección de datos que sean necesarias desde la fase inicial de cualquier planificación y para cualquier desarrollo tecnológico y, en palabras del propio Reglamento, tanto desde el momento de determinar los medios de tratamiento como en el momento del propio tratamiento. Estas medidas, que deberán aplicar desde el primer momento de cualquier proyecto, deberán consistir en medidas técnicas y organizativas apropiadas para dar puntual cumplimiento a los requisitos del Reglamento. Su fin último será el de proteger los derechos de los interesados (sirvan como ejemplos la seudonimización o la minimización de datos). Por su parte, la protección de datos «por defecto» consiste en que el responsable del tratamiento aplique las medidas

20. Estos conceptos son habitualmente referidos por sus denominaciones en lengua inglesa: La violación de seguridad como *Data Breach*, la Privacidad desde el diseño y por defecto como *Privacy by Design* y *Privacy by Default* y la figura del Delegado de Protección de Datos, conocida popularmente como DPO, «*Data Protection Officer*».

técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

El nombramiento de un DPO constituye uno de los elementos claves del Reglamento y un garante del cumplimiento de la normativa de la protección de datos en las organizaciones. El DPO deberá contar con conocimientos en Derecho sin que sea necesario que sea abogado pero obviamente se tratará con de un profesional con amplios conocimientos y experiencia específicos en materia de protección de datos. Su actuación será independiente y reportando a la más alta dirección estando sus funciones reguladas; al DPO corresponde informar y asesorar, así como supervisar el cumplimiento del Reglamento por parte del responsable o encargado.

Igualmente, el Reglamento viene a establecer una serie de nuevos derechos de los interesados como son, por ejemplo, el derecho al olvido, la portabilidad y la limitación del tratamiento así como a reforzar el contenido y la protección asignada a determinados derechos ya existentes como el derecho de acceso. El derecho al olvido significa que el interesado tendrá derecho a obtener, sin dilación indebida y del responsable del tratamiento, la supresión de los datos personales que le conciernan. El responsable estará obligado a suprimir sin dilación indebida los datos personales cuando concurra algunas circunstancias, tales como, que ya no sean necesarios en relación con los fines para los que fueron recogidos, no prevalezcan otros motivos legítimos para el tratamiento o que los datos personales hayan sido tratados ilícitamente.

El derecho a la portabilidad es una forma evolucionada del ya existente derecho de acceso (ver referencia posterior a este derecho) por el cual se otorga la opción a las personas de obtener los datos que han proporcionado a una entidad/empresa/organización (responsable del tratamiento). La copia que se debe proporcionar al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica y, además, se transmiten directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.

La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían. En cuanto al mencionado reforzamiento del derecho de acceso comentar que ya no es suficiente para las empresas a los efectos de dar cumplimiento al mismo con facilitar los datos al interesado sino que éste tiene derecho a obtener una copia de los datos personales objeto del tratamiento.

El régimen de sanciones se ve incrementado significativamente estableciendo sanciones administrativas de hasta 20 millones de euros o el 4% del volumen de negocio total anual global durante el ejercicio anterior.

Finalmente, el 5 de diciembre de 2018 fue aprobada la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Esta norma tiene como objeto adecuar la legislación española al Reglamento. Si bien es cierto que al tratarse de un Reglamento no necesitaba de trasposición ni desarrollo alguno, resultaba absolutamente necesario contar con una regulación nacional que asegurara la adecuación de nuestro marco legal a las directrices de dicho Reglamen-

to. La Ley Orgánica 15/1999 no es a día de hoy suficiente ni adecuada a tal efecto. Señalemos y destaquemos brevemente algunas de las cuestiones que se incluyen en esta normativa nacional.

- Dentro del margen de edad mínima entre 13 y 16 que establece el Reglamento, se sitúa en los catorce años la edad de consentimiento para el tratamiento de datos.
- Se establece y regula el modo de información a las personas acerca del tratamiento de sus datos y, específicamente en el ámbito de internet, se acepta y opta por un sistema de información por capas.
- Consagración y regulación más detallada del derecho al olvido y tanto respecto de motores de búsqueda como de los servicios de redes sociales y servicios equivalentes.
- La Ley incorpora un Título relativo a «Garantía de los derechos digitales», a fin de reconocer y garantizar una serie derechos digitales a los ciudadanos y de los que destacamos los siguientes:
  - Se establecen las garantías del derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo así como el derecho a la intimidad en relación con el uso de dispositivos digitales puestos a disposición de los empleados.
  - La utilización de sistemas de geolocalización en el ámbito laboral exige de información.
- Se establece el correspondiente régimen de infracciones y sanciones tratando de adecuar el mismo a las disposiciones del Reglamento.

III. Normativa relativa a la Sociedad de Servicios de la Información. Cookies y Comunicaciones Comerciales

El punto de partida es la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior y conocida como la Directiva de Comercio Electrónico. Resultado de esta Directiva y como trasposición de la misma fue promulgada la Ley 34/2002 de 11 de julio de Sociedad de la Información y Comercio Electrónico (conocida comúnmente como la «LSSI»). Se entienden comprendidos en el ámbito de aplicación de la LSSI tanto los servicios de la sociedad de la información (tales como, contratación de bienes o servicios por vía electrónica, organización y gestión de subastas por medios electrónicos, envío de comunicaciones comerciales, etc.), como la prestación de servicios de intermediación (acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, etc.).

Conjuntamente con las obligaciones aplicables a los mencionados prestadores de servicios, la norma incluyó un régimen de regulación de los contratos electrónicos y el envío de comunicaciones comerciales por medios electrónicos. Como no podía ser de otra manera, la LSSI también contiene un régimen propio sancionador de aplicación a los prestadores de servicios.

En particular y por su importancia nos centraremos en la regulación establecida en la LSSI sobre el envío de comunicaciones comerciales vía correo electrónico u otros medios equivalentes de comunicación electrónica, como pueden ser los mensajes de móviles (SMS/MMS) así como respecto del uso de dispositivos de almacenamiento y recuperación de datos (conocidos comúnmente por su nomenclatura en lengua inglesa «Cookies»).

a. Las Cookies

Como se ha mencionado, la regulación de Cookies encuentra su origen en la LSSI y, más en concreto, en la modificación que respecto de la redacción de su art. 22 introdujo la ya derogada Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y que vino a trasponer a nuestro ordenamiento numerosa normativa europea de distinta naturaleza relacionada con las telecomunicaciones, la protección de datos y la sociedad de la información. En materia de Cookies vino a implementar, principalmente, los principios fijados por la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

La redacción inicial del art. 22 LSSI contemplaba que «*Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito*». La LSSI y, en concreto, la regulación sobre Cookies, ha sido objeto de varias modificaciones. La primera reforma vino de la mano del Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas. El mencionado Real Decreto-Ley traspuso al ordenamiento español la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre y la Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre[21]. Las cuestiones que a continuación se señalan son el resultado de las reformas mencionadas : (i) las páginas web relativas a estos servicios deben contener información detallada sobre el uso de Cookies y la finalidad de las mismas e incluso que, en determinados casos, el uso de Cookies requiera el consentimiento previa información facilitada a los destinatarios (ii) la regulación se extiende a cualquier dispositivo terminal que utilice Cookies u otros mecanismos de almacenamiento y recuperación de información similares. Por tanto, no solo se refiere a los clásicos computadores de mesa o portátiles (PCs) sino también a otros dispositivos, tales como, smartphones, tablets, móviles o cualquier otro dispositivo que permita acceso a Internet y (iii) la norma aplica no solo respecto de las Cookies propias sino también de

21. Las denominaciones completas de estas Directivas son: (i) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de Comunicaciones electrónicas, 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 el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores y (ii) Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónica, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

las Cookies de terceros, en la medida en que operen en webs propias del prestador o intermediador.

El 9 de mayo de 2014, se aprobó la Ley 9/2014 de Telecomunicaciones que, derogando la Ley 2003, vino a modificar de nuevo y significativamente la regulación sobre Cookies. Entre las modificaciones introducidas, llamamos especialmente la atención sobre las siguientes: (i) suprimió la necesidad de que el usuario deba realizar una acción expresa a través del navegador para entender que ha prestado su consentimiento para la instalación de las Cookies y (ii) extendió la aplicación del régimen de responsabilidad a la red publicitaria o agente que gestione directamente la colocación de anuncios en espacios a tal fin y no solo al prestador del servicio.

i. Concepto y finalidad

Las Cookies, habitualmente, consisten en ficheros o archivos de texto que se instalan en el equipo terminal que esté utilizando en ese momento, ya sea su PC, portátil, Tablet o Smartphone, etc. No obstante, hemos de recordar que si bien por razones de estilo se acude al término Cookies para referirnos con carácter general a todo dispositivo que permita el almacenamiento y recuperación de datos en equipos terminales de usuarios, debemos entender incluido en dicho término todo dispositivo de tales características, sea o no una Cookie en puridad.

Cuando hablamos de la información almacenada en los dispositivos de recuperación de datos lo hacemos en un sentido amplio, ya que no tiene que tratarse (o al menos exclusivamente) de datos de carácter personal. En este sentido, debemos partir de la base de que las obligaciones contenidas en el art. 22.2 LSSI, están vinculadas a la protección de un campo que se considera como parte de la esfera privada del usuario y no al hecho de que la información consista o no en datos de carácter personal. Tal y como ponía de manifiesto la AEPD en la introducción de su Guía sobre el uso de las cookies (en adelante, la «Guía de Cookies[22]»), así como en la resolución de su segundo procedimiento sancionador en relación con la regulación de las Cookies[23] : *«(...) en muchos casos los usuarios que utilizan los servicios de Internet desconocen que el acceso a los mismos puede conllevar la instalación de ficheros o archivos en sus equipos terminales, y que al ser recuperados con la información almacenada en los mismos permiten no solo mejorar la navegación y prestar correctamente el servicio solicitado sino que también posibilitan, con las implicaciones para la privacidad de los usuarios que ello supone, la recogida actualizada y continuada de datos relacionados con sus equipos y perfiles de navegación, que posteriormente podrán ser utilizados por los responsables de los sitios web a los que se accede, o por los terceros, para analizar su comportamiento y para el envío de publicidad basada en el mismo o como medio para el desarrollo de otros productos y servicios concretos. Por lo tanto, para garantizar la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados, que con mayor frecuencia recurren a Internet para la realización de sus actividades cotidianas, la regulación comunitaria y nacional establece*

22. Se refiere a la Guía sobre el uso de las cookies, presentada por la AEPD el 29 de abril de 2013, que supuso la primera guía que regula la aplicación práctica de la normativa de Cookies en Europa elaborada conjuntamente por una autoridad de protección de datos y los representantes de la industria (Adigital, Autocontrol e IAB Spain).

23. Resolución R/00936/2014, en relación con el Procedimiento Sancionador PS/00320/2013, contra Google Inc. por las Cookies que se instalan en sus servicios de *blogs*.

la obtención de un consentimiento informado con el fin de asegurar que estos puedan conocer del uso de sus datos y las finalidades para las que son utilizados».

ii. Implementación de las obligaciones establecidas en la normativa de Cookies[24]

A la hora de afrontar la implementación de los requisitos establecidos en la normativa en el servicio de la sociedad de la información del que seamos responsables, de nuestra experiencia en la materia, podemos afirmar que nunca se debe perder de vista la necesaria colaboración multidisciplinar entre distintos departamentos y personal de una organización. Por ello, se hace imprescindible para lograr nuestro objetivo de cumplimiento normativo, de un lado, la colaboración del área de sistemas o informático para controlar los aspectos relacionados con las tecnologías de la información. De otro, la participación del área jurídica y/o de protección de datos/privacidad, que a través de una interpretación completa y sistemática de la normativa, llegue a unos textos legales ajustados a los requisitos. Finalmente, aunque no menos relevante, mencionar el componente organizativo en el que participarán las áreas antes mencionadas, así como, según los casos, las áreas de Organización, Marketing, Comunicación, etc. a los efectos de fijar los procedimientos internos necesarios.

Teniendo en cuenta lo anterior, el objetivo de cualquier empresa con responsabilidad en el cumplimiento de la normativa de Cookies, será analizar toda la información disponible sobre las obligaciones a cumplir para poder adaptarlas a la realidad del negocio.

24. Como herramientas para hacer frente al cumplimiento señalamos las siguientes:
- Opinion 04/2012 on Cookie Consent Exemption, aprobada el 7 de junio de 2012, del Grupo de Trabajo del art. 29: en la que describen las Cookies que se entienden exceptuadas del cumplimiento de las obligaciones de información y consentimiento recogidas en el art. 5.3 de la Directiva sobre la privacidad y las comunicaciones electrónicas.
- Working Document 02/2013 providing guidance on obtaining consent for cookies, de 2 de octubre de 2013, del Grupo de Trabajo del art. 29: en el que se trata cómo tiene que ser la implementación para cumplir desde el punto de vista legal con la normativa de Cookies.
- Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerpritning, aprobada el 25 de noviembre de 2014, del Grupo de Trabajo del art. 29: en el que se recuerda que el art. 5.3 de la Directiva sobre privacidad y las comunicaciones electrónicas.
- Guía de Cookies de la AEPD: proporciona a las empresas y a los responsables de páginas web en general unas directrices y orientaciones prácticas que facilitan el cumplimiento de las obligaciones legales fundamentales impuestas por la normativa española y que son, en términos generales, el deber de información al usuario y la obtención del consentimiento por parte de este.
- Las resoluciones e informes jurídicos publicados por la AEPD. Resulta a tal efecto material de referencia todo el incluido en el sitio web de la AEPD. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/cookies/index-ides-idphp.php*.
- Otras recomendaciones o instrucciones de las autoridades de países miembros de la Unión Europea y entre las que destacan el ejemplo de Reino Unido, con la «*Guidance on the rules on use of cookies and similar technologie*s» del Information Commissioners Office pioneros en el desarrollo de la normativa de Cookies (*http://ico.org.uk/for_organisations/privacy_and_electronic_communications/ the_guide/cookies*); la publicación de la autoridad francesa (CNIL), Délibération n° 2013-378 du *5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier* 1978; o el caso de Italia en la que el Garante per la Protezione dei Dati Personali publico el 8 de mayo de 2014 los «*Simplifi ed Arrangements to Provide Information and Obtain Consent Regarding Cookie*s».

iii. Tipologías de Cookies

Localizar y categorizar las Cookies que se instalen en cada momento al acceder al sitio web, o utilizar la aplicación móvil, etc., es un paso imprescindible para poder cumplir con las obligaciones de información y consentimiento y requiere colaborar intensamente con el equipo técnico del editor en cuestión o de terceros colaboradores.

La Guía de Cookies, siguiendo el criterio del Grupo de Trabajo del art. 29, recoge una clasificación de los tipos de Cookies que, en términos prácticos nos lleva a lo siguiente:

Cookies exentas

Se trata de aquellas que permitan únicamente la comunicación entre el equipo del usuario y la red o bien resulten estrictamente necesarias para la prestación de un servicio que el usuario ha solicitado expresamente.

Las Cookies técnicas y de personalización suelen tratarse de «entrada del usuario», autenticación o identificación de usuario (limitadas a la sesión), seguridad del usuario, de sesión de reproductor multimedia, de sesión para equilibrar la carga, de personalización de la interfaz de usuario, de complemento (plug-in) para intercambiar contenidos sociales.

El hecho de que se consideren Cookies exentas, viene marcado en muchas ocasiones por la duración (a mayor duración se consideran más intrusivas en términos de privacidad), por lo que esta deberá seguir siempre un criterio de mínimo necesario. Destaca el caso de derecho comparado respecto a Francia, donde la autoridad francesa de protección de datos, Commission Nationale de l'Informatique et des Libertés[25] estableció una duración máxima de 13 meses para la caducidad de las Cookies.

Cookies no exentas

La información que se necesita recabar de las Cookies a las que se deben aplicar los requisitos del art. 22.2 LSSI, requerirá la colaboración de su equipo técnico, así como de aquellos departamentos que puedan llegar a configurar el sitio web para que se carguen Cookies en los terminales de los usuarios, como los Departamentos de Sistemas, Marketing, etc. Recordamos la necesidad de que, cuando se instalen Cookies de terceros, se refleje la identidad de dicho tercero o terceros que van a acceder a la información del usuario. En este sentido, debemos destacar que la interpretación de la AEPD de la normativa de Cookies se antoja más detallada en este requisito de información que la estricta normativa de protección de datos (en la que no se exige al responsable del fichero o tratamiento identificar al prestador de servicios concreto en la información facilitada al interesado o afectado).

En relación con esta cuestión, la AEPD señaló en su Resolución 02990/2013, respecto del PS/00321/2013 la falta de información adecuada que no se identifique al tercero prestador: «[...] *Por lo tanto, no contiene una información adecuada sobre el tipo de cookies que efectivamente se utilizan y sus finalidades que permita conocer*

25. Entidad regulatoria comúnmente conocida y referida por sus siglas: «CNIL»

al usuario de una forma apropiada el uso que se dará a la información recuperada, tampoco se asocia claramente su uso con el propio editor o con terceros que también deben ser identificados [...]».

Sobre la base de lo anterior, recogemos a continuación una posible solución práctica de la información que debe conocer internamente un editor de sitio web sobre las Cookies, a través de un cuadro en el que la parte sombreada con la descripción de los tipos de Cookies permanezca fija, y la blanca se edite para incluir las concretas Cookies no exentas en función de su finalidad, y la información sobre Cookies según el plazo de tiempo que permanecen activas (de Sesión/Persistentes) y la entidad que las gestione (Propias o de Tercero):

Cookies de análisis: *Permiten al responsable el seguimiento y análisis del comportamiento de los usuarios del sitio web. La información recogida se utiliza para la medición de la actividad del sitio web, y para la elaboración de perfiles de navegación del usuario en el sitio web para introducir mejoras en función del análisis de los datos de uso del servicio por los usuarios.*			
Incorporar dominio bajo el que figura la Cookie así como el nombre técnico o identificador de la Cookie para tratar de localizar las Cookies que se instalen.	*Descripción de la finalidad concreta para la que se tratan los datos obtenidos del usuario y forma de la que se lleva a cabo por el Editor o un tercero.*	*Indicar si se trata de una Cookie de Sesión o Persistente (y como información a valorar internamente, el plazo de caducidad).*	*Indicar si se trata de una Cookie propia o de tercero (en cuyo caso, se identificará al prestador).*
Cookies publicitarias: *Permiten la gestión eficaz de los espacios publicitarios del sitio web sobre la base de criterios de como el contenido editado o la frecuencia en la que se muestran los anuncios.*			
Dominio bajo el que figura y nombre técnico de la Cookie	*Descripción de la finalidad.*	*Cookie de Sesión o Persistente.*	*Cookie propia o de tercero (identificado).*
Cookies de publicidad comportamental: *Permiten la gestión eficaz de los espacios publicitarios del sitio web sobre la base de criterios de como el contenido editado o la frecuencia en la que se muestran los anuncios. Este tipo de cookies almacenan información del comportamiento de los usuarios obtenida a través de la observación de sus hábitos de navegación, por lo que se desarrollan perfiles específicos para mostrar publicidad en función del mismo.*			
Dominio bajo el que figura y nombre técnico de la Cookie	*Descripción de la finalidad.*	*Cookie de Sesión o Persistente.*	*Cookie propia o de tercero (identificado).*

De forma específica, bajo la perspectiva de la AEPD, las Cookies de análisis que sean propias y solo traten datos agregados, pese a considerarse menos invasivas, no se encuentran exentas de aplicación del art. 22.2 LSSI.

Una cuestión práctica que no debemos perder de vista es la necesidad de realizar este ejercicio de localización y documentación de las Cookies de manera periódica.

b. Las Comunicaciones Comerciales

Un muy breve esbozo de la regulación relativa a las comunicaciones comerciales. En relación con esta cuestión la LSSI establece que éstas deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable estando específicamente prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación. Igualmente queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente salvo que previamente hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. En cuanto al consentimiento para el envió de comunicaciones comerciales es importante volver a recalcar el impacto que en esta cuestión tiene la nueva regulación al respecto que se contiene en el Reglamento.

En cualquier caso y en línea con la preocupación por la protección de los usuarios en esta materia, la LSSI dispone expresamente que el destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente y, a tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos (por ejemplo, si las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida).

Como se ha indicado, todas las normativas vistas hasta este punto del trabajo están íntimamente interrelacionadas y constituyen la regulación esencial (que no única) a tener en cuenta en materia de comercio electrónico. Prueba evidente y «visual» de esto es que la propia LSSI matiza que lo dispuesto en la LSSI se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo y de la regulación específica en materia de Protección de Datos[26].

26. Además de otras referenciadas a lo largo del presente Capítulo, incluimos una mención a ciertas guías y sitios web de gran utilidad y referencia a los efectos de lo aquí tratado.

«Guía para una Evaluación del Impacto en la Protección de Datos Personales (EIPD)», «Guía para La Lucha Contra el Spam» y «Guía sobre Privacidad y Seguridad en Internet» y publicadas por la AEPD.

«Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978» publicada por el CNIL.

«Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies», del Garante Italiano.

- *http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf*
- *www.enisa.europa.eu*
- *www.inteco.es*

IV. Breve referencia a la normativa bancaria y al estándar de seguridad «PCI-DSS»

Indicamos a continuación y a modo de mera mención la normativa bancaria y con especial incidencia en lo relativo a pagos y cobros. Cuestión ésta esencial en materia de Comercio Electrónico.

En el ámbito de la Unión Europea resultan especialmente importantes los siguientes Reglamento y Directiva:

- Reglamento (UE) No 260/2012[27]; su ámbito de aplicación se encuentra limitado a transferencias bancarias y adeudos domiciliados y no regula pagos con tarjeta.
- Directiva (UE) 2015/2366[28] que ha venido a sustituir a la Directiva (UE) 2007/64/CE6, de 13 de noviembre de 2007 y que estuvo vigente hasta el 13 de enero de 2018. Esta Directiva dota de regulación a los instrumentos de pago en el ámbito de la Unión Europea, entre ellos las tarjetas de crédito.

En España, y como resultado de trasponer la normativa anterior, debemos mencionar la Ley 16/2009, de 13 de noviembre, de servicios de pago y la Orden EHA/1608/2010, de 14 de junio, sobre transparencia de las condiciones y requisitos de información aplicables a los servicios de pago[29].

Por su relevancia y presencia en el mercado, creemos también importante dedicar una parte de este trabajo al estándar de seguridad en los datos de tarjetas bancarias denominado PCI-DSS. Se trata de un estándar de seguridad desarrollado por el *Payment Card Industry Security Standards Council* (PCI-SSC) que es un consorcio que aglutina a American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa International Inc. PCI-DSS no es en sí una ley, si bien en algunos países existen leyes con requerimientos similares a algunos de los de PCI-DSS[30] o que, directamente, establecen como obligatorio el cumplimiento de PCI-DSS. Además, su incumplimiento puede conllevar sanciones por parte de las entidades financieras y/o de las marcas de tarjetas.

La finalidad de este estándar es combatir las transacciones con tarjetas bancarias fraudulentas y aumentar la seguridad de los datos almacenados en ellas. Las entidades anteriormente mencionadas y miembros del consorcio han adoptado este estándar como los requisitos a demandar de los comerciantes y otros operadores, proveedores u organizaciones que, en su caso, almacenen, transmitan o procesen información sobre tarjetas bancarias y/o de sus titulares.

27. La referencia completa es Reglamento (UE) nº 260/2012 del Parlamento Europeo y del Consejo de 14 de marzo de 2012, por el que se establecen requisitos técnicos y empresariales para las transferencias y los adeudos domiciliados en euros, y se modifica el Reglamento (CE) nº 924/2009 (DOUE de 30 de marzo).

28. La referencia completa es Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE.

29. Por su utilidad recomendamos el siguiente link dentro de la Web del Banco de España donde se puede encontrar una relación más completa de la normativa aplicable en esta materia: *https://www.bde.es/bde/es/secciones/normativas/Regulacion_de_En/Comunitaria/Sistemas_y_servicios_de_pago.html*

30. Por ejemplo, en Estados Unidos la ley *Foreign Account Tax Compliance Act* y conocida comúnmente y por sus siglas como «*FACTA*».

Los requisitos y obligaciones regulados pretenden establecer prácticas, procedimientos y cautelas a los comerciantes, proveedores de servicios de pagos u otros operadores afectados para que éstas aseguren que sus herramientas tecnológicas, software, procedimientos, arquitecturas tecnológicas e infraestructuras sean adecuadas para proteger los datos de los titulares de tarjetas.

PCI-DSS contiene 246 requerimientos agrupados en 12 secciones. La mayoría son técnicos, aunque también incluye muchos operativos (tratamiento de datos, gestión de proveedores, etc.) y documentales. Sirva la siguiente tabla de referencia al respecto.

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Desarrolle y mantenga redes y sistemas seguros.	**1.** Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta. **2.** No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta	**3.** Proteja los datos del titular de la tarjeta que fueron almacenados **4.** Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	**5.** Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente. **6.** Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	**7.** Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. **8.** Identificar y autenticar el acceso a los componentes del sistema. **9.** Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	**10.** Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta **11.** Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	**12.** Mantener una política que aborde la seguridad de la información para todo el personal

Además de lo anterior, es importante mencionar que PCI-DSS incluye varios requerimientos relacionados con la gestión de proveedores y que pueden resumirse en los siguientes:

- Mantener una lista de proveedores de servicios incluyendo una descripción de los servicios prestados relacionados con los datos de tarjetas.
- Mantener un contrato escrito que incluya un reconocimiento de que los proveedores de servicio son responsables de la seguridad de los datos de los titulares de tarjetas que poseen o bien almacenan, procesan o transmiten en nombre del cliente, o en la medida que puedan impactar en la seguridad del entorno de los datos del titular de tarjeta de los clientes.
- Establecer un proceso de análisis del cumplimiento del proveedor antes de su contratación.
- Monitorizar anualmente el estado de cumplimiento de PCI DSS de cada proveedor de servicio.
- Documentar qué requerimientos de PCI DSS son gestionados por cada proveedor y cuáles por el Comercio.

En cuanto al alcance de aplicación, hay que tener en cuenta que PCI-DSS es el estándar de seguridad común aplicable a nivel mundial, siendo especialmente relevante en el ámbito de la Unión Europea y América.

No obstante, en otros mercados críticos en el Comercio Electrónico (por ejemplo, China, Japón o Corea), si bien las marcas mencionadas obviamente también requieren dichos cumplimientos, los bancos parecen ser menos exigentes respecto de PCI-DSS. Ello debido a la menor presencia de las marcas internacionales y la mayor presencia y relevancia de las tarjetas «domésticas».

V. Derecho de la Competencia. Actuaciones y nuevas regulaciones sobre geobloqueo

La incidencia del Derecho de la Competencia, al igual que respecto de cualquier otra actividad económica o actuación en el tráfico mercantil, es de una gran relevancia en el Comercio Electrónico. Por ello, merece siempre y con carácter previo a cualquier operación o actuación, llevar a cabo un análisis profundo y pormenorizado de todas las posibles implicaciones que desde el punto de vista del Derecho de Competencia (nacional y/o extranjero –y ya sea entorno UE como fuera del mismo–) puedan afectar al sitio web, su lanzamiento, sus contratos, etc. Así, creemos que las cuestiones que más recurrentemente pueden afectar al Comercio Electrónico son, entre otras, las siguientes; abuso de posición de dominio, acuerdos de distribución selectiva, compras activas y pasivas, integraciones en plataformas de terceros y distribución selectiva así como las relativas a discriminaciones por cuestiones geográficas. De todas estas cuestiones y por su especial actualidad, particularidad y relevancia nos vamos a centrar en la última de ellas (esto es, las relativas al bloqueo geográfico).

Al igual que mencionamos cuando hablamos del acceso de los consumidores a mecanismos de resolución de conflictos por medios alternativos, la Unión Europea[31] viene considerando, como otra parte esencial de la estrategia para alcanzar un Mercado Único (y en este caso un Mercado Único «Digital»), el abordar y mitigar el bloqueo geográfico no justificado. Entiéndase a estos efectos como bloqueo geográfico no justificado como la segmentación artificial del mercado interior por la discriminación directa o indirecta por razón de nacionalidad, lugar de residencia o lugar de establecimiento de los clientes.

La normativa Europea[32] y los diferentes desarrollos normativos nacionales relativos a la sociedad de la información autorizan a los comerciantes a llevar a cabo y en línea operaciones transfronterizas y prestar sus servicios sobre la base de normas aplicables en su país de establecimiento. Sin embargo, también establece como principio esencial que los proveedores de servicios establecidos en la Unión no den un trato diferente a los clientes por razón de su nacionalidad o su lugar de residencia, ni directa ni indirectamente. No obstante, la propia Unión Europea reconoció que, a pesar de la potenciación del principio señalado, no se habían regulado suficientemente

31. La Estrategia para el Mercado Único Digital de Europa (COM 2015 –192– final), adoptada en mayo de 2015, y la Estrategia del Mercado Único (COM 2015-550-final), adoptada en octubre de 2015, anunciaron medidas legislativas para abordar el bloqueo geográfico injustificado y luchar de forma integral contra la discriminación por razón de la nacionalidad o del lugar de residencia o de establecimiento.

32. Nos referimos principalmente a la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

las cuestiones relativas a discriminación de los clientes y que ello había generado una gran inseguridad jurídica. Inseguridad jurídica tanto para los comerciantes y sus clientes como para otros operadores. Dicho de otro modo, hasta la aprobación del Reglamento sobre geobloqueo que mencionaremos a continuación no existían directrices claras o regulaciones sobre que técnicas o actuaciones en el mundo de la venta en línea constituyen actuaciones susceptibles de ser catalogadas como discriminatorias por razón de residencia y cuáles no.

Fruto de la mencionada preocupación, la Comisión Europea llevó a cabo un trabajo de investigación y análisis durante el año 2015 a través de la realización de diversas encuestas y consultas públicas como, por ejemplo, la consulta sobre geoblocking[33] y que se contemplaba conjuntamente con un proceso de investigación[34] sobre la competencia en el sector del comercio electrónico. En concreto, La finalidad de dicho estudio sectorial consistía en recopilar datos acerca del funcionamiento de los mercados del comercio electrónico y en detectar posibles problemas de competencia, particularmente en el ámbito del comercio electrónico transfronterizo.

En mayo de 2016 y sobre la base de la información obtenida, la Comisión Europea presentó una propuesta de regulación sobre el bloqueo geográfico, acompañada de propuestas legislativas complementarias relativas a los servicios de paquetería transfronterizos y de una versión revisada del Reglamento sobre cooperación en materia de protección de los consumidores. El objetivo de estas iniciativas era avanzar hacia la integración de un verdadero mercado único.

Finalmente y como consecuencia de todo el proceso descrito, se aprobó por el Parlamento Europeo con fecha 6 de febrero de 2018 y por el Consejo el 27 de febrero de 2018 el Proyecto de Reglamento del Parlamento Europeo y del Consejo sobre las medidas contra el bloqueo geográfico y otras formas de discriminación por razón de la nacionalidad o del lugar de residencia o de establecimiento de los clientes en el mercado interior. Esta normativa ha modificado el Reglamento (CE) n.º 2006/2004 y la Directiva 2009/22/CE y resultará de aplicación a partir del 3 de diciembre de 2018. El mencionado Reglamento tiene como objeto la supresión de limitaciones a la actividad de compra en línea transfronteriza dentro de la Unión Europea que resultan de las prácticas mencionadas y asegurar que, salvo motivos justificados, los consumidores puedan comprar dentro del espacio europeo con las mejores ofertas disponibles en un entorno de mercado único. En palabras de Lilyana Pavlova, Ministra para la Presidencia búlgara del Consejo de la UE; «*el fin del bloqueo geográfico supone que haya donde elegir, mejores ofertas para los consumidores y más oportunidades para las empresas*».

Conforme a la nueva normativa[35] se definen tres casuísticas en que los comerciantes no podrán discriminar entre clientes por lo que se refiere a las condiciones generales, incluidas los precios. Se trata de aquellos casos en que el comerciante:

33. Consulta sobre geo-blocking (*https://ec.europa.eu/eusurvey/runner/geoblocksurvey2015/*).

34. Investigación sobre la competencia en el sector del comercio: *http://ec.europa.eu/competition/antitrust/sector_inquiries_e_commerce.html.*

35. Tras su aprobación y publicación definitiva; Reglamento (UE) 2018/302 del Parlamento y del Consejo de 28 de febrero de 2018 sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior.

- Vende bienes que se entregan en un Estado Miembro en el que el comerciante ofrece servicios de entrega o que se recogen en un lugar acordado con el cliente.
- Presta servicios por medios electrónicos, como los servicios en nube, el depósito de datos, el alojamiento de sitios web y la provisión de cortafuegos.
- Presta servicios que el cliente recibe en el país en el que opera el comerciante, como servicios de alojamiento en hotel, acontecimientos deportivos, alquiler de coches o billetes de entrada a festivales de música o parques de atracciones.

Los comerciantes no podrán, por motivos relacionados con la nacionalidad, el lugar de residencia o el lugar de establecimiento del cliente bloquear o limitar el acceso de los clientes a las interfaces en línea del comerciante utilizando medidas tecnológicas (como por ejemplo geolocalización). Tampoco podrán re-direccionar a clientes sin su consentimiento explícito a una versión de la interfaz en línea del comerciante distinta de la interfaz en línea a la que el cliente haya tratado de acceder inicialmente. Será suficiente con que el consentimiento se otorgue una única vez (sin necesidad por tanto de obtenerlo para futuros re direccionamientos), si bien ha de garantizarse que en todo momento que puede ser revocado.

El cliente de cualquier Estado Miembro debe poder realizar transacciones comerciales en las mismas condiciones que los clientes de los países en cuestión y acceder por igual a los diferentes productos o servicios ofrecidos. Ello independientemente de su nacionalidad, lugar de residencia o lugar de establecimiento temporal o permanente. Esto no afecta al derecho de los comerciantes a aplicar diferentes condiciones en los distintos países como, por ejemplo, los precios. Esta regulación tampoco implica la imposición a los sitios web de realizar entregas transfronterizas de mercancías respecto de otros Estados Miembros.

Se mantiene la libertad de los comerciantes de aceptar cualquier medio de pago. El Reglamento incluye una disposición específica sobre la no discriminación dentro del rango de medios de pago que acepten. Se refiere a aquellas situaciones en las que el tratamiento discriminatorio o diferencial es debido a la nacionalidad del cliente, el lugar de residencia o el lugar de establecimiento del cliente, la ubicación de la cuenta de pago, el lugar de establecimiento del proveedor de servicios de pago o el lugar de expedición de la instrumento de pago. En este sentido, téngase en cuenta que se prohíbe el tratamiento diferencial si se cumplen estas tres condiciones; (i) los pagos se realizan a través de transacciones electrónicas mediante transferencia, adeudo domiciliado o instrumento de pago basado en tarjeta dentro de la misma marca y categoría, (ii) se cumplen los requisitos de autenticación (en concreto, los contemplados la Directiva (UE) 2015/2366) y (iii) los pagos se encuentran en una divisa que el comerciante acepta. Las restricciones a las ventas pasivas se siguen considerando una vulneración del Derecho de la competencia y este principio se mantiene. En cuanto a las ventas activas, el Reglamento no afecta a la regulación del derecho de los comerciantes a imponer restricciones a estas ventas[36].

36. El Derecho de competencia distingue entre ventas pasivas (las realizadas en respuesta a solicitudes espontáneas) y las ventas activas (las que realizan los minoristas cuando captan activamente a los clientes).

4. NUEVAS NORMATIVAS RELEVANTES EN RUSIA Y CHINA

Como anticipábamos en la Introducción, se han aprobado en Rusia y China dos normativas con un gran impacto en los sitios web nacionales y extranjeros que operen o quieran operar en estos mercados estratégicos. En el caso de Rusia, en relación con el tratamiento de datos que afecten a ciudadanos rusos y, en el de China, en materia de Ciberseguridad. A pesar de que son normas que se han promulgado y entrado en vigor en los años 2014 y 2017, podemos seguir predicando de ellas que son recientes y actuales. Ello es debido a su complejidad y el mencionado impacto en las compañías. De hecho, a fecha de hoy, siguen siendo objeto de reformas, normas de desarrollo e interpretaciones por los reguladores. Como decimos, son de máxima actualidad si, además de lo señalado y principalmente, tenemos en cuenta que siguen estando sometidas a un profundo análisis sobre sus consecuencias prácticas, los costes de implementación y el aseguramiento de su cumplimiento por las empresas afectadas.

I. Rusia y el almacenamiento, tratamiento y localización de datos

El 4 de julio de 2014, la Duma de la Federación Rusa adoptó una serie de acuerdos normativos que derivaron finalmente en la promulgación de la Ley Federal No 242-FZ sobre Modificaciones en Ciertas Legislaciones de la Federación Rusia para la Regulación del Procedimiento para el Tratamiento de Datos Personales en las Redes de Telecomunicaciones[37] (en adelante, la «Ley Federal No 242-FZ»). Esta norma supuso la inclusión de varios requisitos y medidas en relación con el almacenamiento de datos y su tratamiento cuando afectan a ciudadanos rusos.

Los nuevos requisitos se podrían resumir como sigue. Se establece el deber de garantizar que los datos personales de los ciudadanos rusos serán recabados, registrados, sistematizados, acumulados, almacenados, especificados (actualizados o modificados) y obtenidos en bases de datos y servidores ubicados en Rusia. Es indiferente si los datos personales se recaban en línea o por cualquier otro medio. Los operadores tendrán la obligación de facilitar a las autoridades reguladoras responsables información acerca del lugar donde se ubica la base de datos si contiene datos personales de ciudadanos rusos. En caso de incumplimientos, y además de las posibles sanciones, el Roskomnadzor[38] tendrá derecho a restringir el acceso a dichos datos (incluida la posibilidad de bloquear un sitio web). Esta cuestión afecta principalmente a vulneraciones consistentes en tratamiento de datos personales en bases de datos ubicadas fuera de Rusia. Se acuerda la creación un sistema automatizado y registro en el que se incluirán, respecto de posibles incumplidores e incumplimientos, entre otras cosas, los nombres de dominio y/o los sitios web así como con las direcciones IP que permitan la clara identificación a estos efectos. A fin de poder asegurar lo anterior, se refuerzan las capacidades inspectoras de los órganos reguladores. La idea es que, por ejemplo, el Roskomnadzor pueda actuar con mayor rapidez ante informaciones acerca de posibles vulneraciones y que para hacerlo no tenga o no necesite interactuar efectivamente con los operadores potenciales incumplidores.

37. Traducción de carácter no oficial y a efectos de este documento partiendo de su denominación original en lengua inglesa y rusa.

38. Órgano regulador ruso.

Como últimos avances mencionar que el Roskomnadzor aprobó el 22 de agosto de 2017 una Orden que revisó los protocolos inicialmente concebidos para las notificaciones debidas por las empresas que almacenen o traten datos personales en Rusia. Se ha venido a requerir que estas empresas notifiquen al Roskomnadzor con anticipación sobre el procesamiento de datos personales, incluida información sobre las protecciones existentes para evitar infracciones de datos. Deberá informar igualmente cuando la empresa tenga la intención de transferir datos fuera de Rusia (y, de ser así, los países a los que se transferirán los mismos). Las empresas afectadas también deben confirmar formalmente su conformidad con las disposiciones y requisitos de la Ley Federal No 242-FZ.

II. Nueva regulación sobre ciberseguridad en China (La «CSL[39]»)

La CSL entró en vigor el 1 de junio de 2017 y es la pieza fundamental de la legislación china en materia de ciberseguridad y protección de datos personales. Tras la entrada en vigor de la CSL, las autoridades chinas[40] han publicado varias proposiciones y normativa de desarrollo para aclarar las cuestiones más complejas o relevantes. Se trata, por tanto, de una ley dentro de otra serie de leyes y normativas sobre ésta y otras cuestiones relacionadas.

La CSL se propone reforzar la soberanía sobre su dominio público, recabando, controlando y almacenando información corporativa y personal a la vez que lucha por combatir el fraude en línea. Impulsada como una medida de seguridad pública, su objetivo principal consiste, según su propia indicación, en prevenir toda tentativa tanto externa como interna de «...*propagar la violencia, el terror, falsos rumores, pornografía, y otros riesgos para la seguridad nacional, la seguridad pública y el orden social*.» La CSL afecta directamente a muchas multinacionales extranjeras que operan actualmente en China y permite a las autoridades, de verlo necesario y en aras de lo anterior, acceder a cualquier dato y con independencia de su naturaleza o sensibilidad y de cualquier sociedad.

Algunas de las medidas más relevantes adoptadas son las siguientes:

- La adquisición y el tratamiento de datos personales de todas las sociedades y personas que viven y trabajan en China deberá permanecer en el país en sitios *Host* aprobados por el Gobierno chino. Además, será preceptiva la contratación de proveedores de servicios de *Host* y *Cloud* que cuenten con licencia suficiente y sean aprobados por el Gobierno chino para operar en el país[41].
- Se exige a toda empresa nacional o extranjera que explote un sitio web en China que obtenga la «*Licencia de Proveedor de Contenidos de Internet*»[42].

39. Referenciada así de forma generalizada y por su traducción y siglas en lengua inglesa: *Cyber Security Law of the People's Republic of China.*

40. En concreto, y referenciadas por su traducción a la lengua inglesa: la *Cyberspace Administration of China* y el *National Information Security Standardization Technical Committee.*

41. Tal es el caso de la licencia Internet Data Centre Value-Added Telecom Service *(«IDC VATS»).*

42. Traducción no oficial y libre del término en lengua inglesa y comúnmente usado *Internet Content Provider* (ICP). Se trata de un permiso validado y expedido por el correspondiente órgano Administrativo y de Comunicación de cada Provincia. Aquellas empresas que carezcan del permiso aprobado por el Gobierno o incumplan de algún modo pueden ser bloqueadas, multadas o incluso podrán enfrentarse a un corte permanente de internet.

- Se distinguen dos graduaciones en cuanto a las medidas de seguridad a implementar y régimen de obligaciones en materia de ciberseguridad según se considere que la entidad en cuestión es un «*Network Operator*» o un «*Critical Infraestructure Information Operator* (*CIIO*)»[43]. Esta segunda categoría está sometida a requisitos y obligaciones adicionales respecto del Network Operator. Centrémonos con un poco más de detalle en esta cuestión.

Se consideran Network Operators los operadores o propietarios de redes o administradores o proveedores de servicios en línea. Una definición amplia que podría interpretarse (y, de hecho, así se interpreta) que abarca a cualquier empresa nacional o extranjera que opere en línea en China. Entre otras, las obligaciones de un Network Operator incluyen las siguientes:

- Formulación de un protocolo interno de seguridad y procedimientos operativos.
- Adopción de medidas técnicas para prevenir y mitigar las intrusiones cibernéticas.
- Realización de las pertinentes notificaciones a los usuarios y autoridades reguladoras sobre rupturas de seguridad (*data breaches*).
- Si está proporcionando acceso a Internet, por teléfono o por mensajería (SMS) a los clientes «deberán exigir a los usuarios que proporcionen su identidad real» y denegarán el servicio a los clientes que se nieguen a hacerlo. Esto implica la necesidad, en la práctica, de asegurar procesos técnicos y operativos de autenticación y verificación eficientes a tal efecto.

Se incluye una amplia definición de CIIO y que abarca a los operadores en los siguientes sectores; servicios públicos de comunicación e información, electricidad, transporte, agua, finanzas así como una categoría general a modo de cajón de sastre que amplia significativamente el posible elenco de afectados «*cualquiera que pueda poner en grave peligro la seguridad nacional, la economía nacional, el sustento de las personas o el interés público*». Nuestra interpretación es que aquellas multinacionales que operen en línea y tengan acceso a un volumen significativo de información que afecte al país o sus nacionales, son susceptibles de caer bajo esta categoría.

Adicionalmente a las obligaciones ya impuestas a los Network Operators, los CIIO deberán:

- Establecer departamentos especializados de gestión de la seguridad así como impartir formación continuada y evaluar la capacitación de los empleados en ciberseguridad.
- Realizar copias de seguridad para supuestos de desastre o rupturas y planes de emergencia y respuesta ante dichos escenarios.
- Se somete a los CIIP a controles y evaluaciones por las autoridades competentes.

43. En este caso, nos referirnos a estos conceptos directamente por sus respectivas denominaciones y siglas en lengua inglesa. Ello a fin de evitar innecesarias confusiones y debido a su común y generalizado uso.

- Nombrar un tercero cualificado para llevar a cabo evaluaciones anuales de ciberseguridad y riesgos.
- Cooperar con las autoridades competentes facilitando toda la información necesaria.

5. ¿«NUEVOS»? RETOS PLANTEADOS

Todo lo que en este trabajo hemos descrito, ni trata ni soluciona la problemática legal y, en parte, ya actual, que los continuos avances de la tecnología y sus resultados (nuevas herramientas para el análisis de datos, funcionalidades, fuentes de obtención de información, etc.) están planteando y, sin duda, seguirán planteando en el futuro. En este sentido y como «lista» inicial, no podemos evitar preguntarnos cómo se solucionarán las múltiples «incógnitas» y las lagunas legales que, entre otras muchas, implicarán las cuestiones que más adelante se indican. Desafortunadamente, esta lista y los interrogantes que en ella se formulan son, además de subjetivos, de mínimos. Existen muchísimas otras. Invitamos al lector a llevar a cabo una reflexión similar como ejercicio intelectual posterior a la lectura de este trabajo. Estamos seguros de que le resultará interesante o, incluso, algo inquietante....:

- Big data*: ¿Existe conocimiento y posibilidad alguna de oposición respecto del acceso y uso de datos e información de las personas por los Estados, agencias, grandes compañías...?*
- «Internet of Things»: *¿Somos conscientes de qué dispositivos de nuestro día a día recopilan información nuestra y de nuestro entorno y de qué tipo?*
- Ciberseguridad: *¿Dónde se produce territorialmente el cibercrime (¿Lugar de la IP?, ¿Lugar de comisión del delito? ¿Dónde esté ubicado el servidor? ¿En la Nube – y dónde está la Nube-?)? ¿Cómo se puede «perseguir» de una forma realmente efectiva en la práctica?*
- Criptomonedas: *¿Problemas derivados de altas e inesperadas fluctuaciones o efectos «burbuja»? ¿Aumento de escenarios de fraude?*
- Blockchain: *¿Descentralización, desregulación y anonimidad?*
- Cloud Computing *¿Delimitación de responsabilidades? ¿Quiénes son y donde están localizados los posibles responsables por incumplimientos? ¿Dónde están localizados dichos incumplimientos y sus correspondientes daños en sí?*
- Personalización, analytics, segmentación, publicidad comportamental, etc: *¿Cuáles son los límites entre lo «comercialmente aceptable» y la intrusión en la privacidad?*
- Inteligencia artificial, Impresoras 3D, Realidad Virtual y Aumentada.... *¿Consecuencias desde un punto de vista de su impacto en el empleo y el Derecho laboral? ¿Cuestiones relativas a Propiedad Intelectual e Industrial?*
- Dark Net y Redes TOR *¿Posibles territorios para la impunidad?*
- Firma electrónica: *¿Problemas de prueba? ¿Suplantaciones de identidad?*

- Fintechs, medios de pago y pasarelas de pago virtuales *¿El fin de los bancos y medios de pago como los hemos conocido? ¿Problemas regulatorios? ¿Seguridad en las Transacciones? ¿Gestión de insolvencias?*

BIBLIOGRAFÍA

AGUSTINOY GUILAN, A. y MONCLÚS RUIZ, J., Aspectos Legales de las Redes Sociales, Madrid, Wolters Kluwer, 2016.

ALCOVER GARAU, G., «La firma electrónica como medio de prueba (valoración jurídica de los criptosistemas de claves asimétricas)», Cuadernos de Derecho y Comercio nº 13, 1994.

ALONSO ESPINOSA, F.J., Régimen jurídico general del comercio minorista (Comentarios a la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista, y a la Ley Orgánica 2/1996, complementaria de la de ordenación del comercio minorista), Madrid, McGraw-Hill, 1999.

ALONSO UREBA, A. y VIERA GONZÁLEZ, A.J., «Formación y perfección de los contratos a distancia celebrados por Internet», en R. Mateu de Ros y M. López-Monís Gallego (coordinadores), Derecho de Internet (La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico), Navarra, Aranzadi, 2003.

ALVAREZ-CIENFUEGOS SUAREZ, J.M., La firma y el comercio electrónico en España (Comentarios a la legislación vigente), Navarra, Aranzadi, 2000.

APARICIO SALOM, J., Estudio sobre la Ley Orgánica de protección de datos de carácter personal, Navarra, Aranzadi, 2009.

BANISAR, D. y DAVIES, S., «*Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Law and Developments*» *Journal of Computer & Information Law,* vol. XVIII, 1999, pp. 1-111.

BERMAN, P.S., «*Choice of Law and Jurisdiction on the Internet (Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interest in a Global Era)»,* University of Pennsylvania Law Review, vol. 153, 2005.

CONTRERAS NAVIDAD, S., La protección del honor, la intimidad y la propia imagen de Internet, Navarra, Aranzadi, 2012.

DE MIGUEL ASENSIO, P., Derecho Privado de Internet, Navarra, Aranzadi, 2015.

DELGADO MARTÍN, J., «Responsabilidad penal de los proveedores de servicios de la sociedad de la información. Especial referencia a las páginas web de enlace», Diario La Ley, núm. 8254, de 19 de febrero de 2014.

DESANTES REAL, M., «La Directiva sobre el comercio electrónico. Mercado interior y servicios de la sociedad de la información», R. Mateu de Ros, J. M. Cendoya (coordinadores), Derecho de Internet (Contratación electrónica y firma digital), Navarra, Aranzadi, 2000.

ÉCIJA BERNAL, A. y SAIZ PEÑA, C.A. (coordinadores), Contratos de Internet (Modelos y comentarios prácticos), Navarra, Aranzadi, 2002.

FERNÁNDEZ ESTEBAN, M.L., Nuevas tecnologías, Internet y derechos fundamentales, Madrid, McGraw-Hill, 1998.

FERRERES COMELLA, A., «Las Acciones de Clase («Class Actions») en la Ley de Enjuiciamiento Civil», Madrid, Actualidad Jurídica Uría y Menéndez, 2005.

FLEISCHMANN, A., «*Personal Data Security: Divergent Standards in the European Union and the United States*», Fordham I.L.J., vol. 19, 1995.

GÓMEZ TOMILLO, M., Responsabilidad penal y civil por delitos cometidos a través de Internet. (Especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces), Navarra, Aranzadi, 2006.

GONZÁLEZ GOZALO, A., La formación del contrato tras la Ley de servicios de la sociedad de la información y comercio electrónico, Granada, Comares, 2004.

GONZÁLEZ PACANOWSKA, I., «Artículo 9», F. J. Alonso Espinosa y otros (coordinadores), Régimen jurídico general del comercio minorista, Madrid, McGraw-Hill, 1999.

HILL, R., *The New International Telecommunication Regulations and the Internet*, Heidelbeg, Springer, 2014.

ILLESCAS ORTIZ, R., Derecho de la contratación electrónica., Navarra, Civitas Thomson Reuters, 2009.

JOINT, A., Selling Cyberspace: New Legal Issues Emerge as the Online Advertising Industry Continues to Grow», Computer Law Security Report, vol. 19, 2003.

JULIÁ BARCELÓ, R., Comercio electrónico entre empresarios (La formación y prueba del comercio electrónico), Valencia, Tirant lo Blanch, 2000.

KOHL, U., *Jurisdiction and the Internet (Regulatory competence over online activity)*, Cambridge, Cambridge University Press, 2007.

LÓPEZ JIMÉNEZ, D., «La Contratación Electrónica a través de Dispositivos móviles: un examen multidisciplinar». Revista Internacional del Mundo Económico y del Derecho. Chile, Volumen VI, 2013.

MADRID PARRA, A., Derecho patrimonial y tecnología, Madrid, Marcial Pons, 2007.

OLTRA GUTIÉRREZ, J., Impacto legal de la informática en las organizaciones. Valencia, Universidad Politécnica de Valencia, 1999.

PEGUERA POCH, M., La exclusión de responsabilidad de los intermediarios en Internet, Granada, Comares, 2007.

PIÑAR MAÑAS, J.L., «El porqué de un Reglamento de desarrollo de la Ley Orgánica de Protección de Datos», Revista Española de Protección de Datos, nº 3, 2007.

SANCHO VILLA, D., Negocios internacionales de tratamiento de datos personales, Madrid, Civitas, 2010.

SERRANO ACITORES, A., LOPEZ DE LA OSA, P., TORAL OROPESA, P., y VELASCO FABRA, G., (coordinadores), La intervención administrativa y económica en la actividad empresarial, Madrid, Wolters Kluwer, 2015.

VILLAR URÍBARRI, J.M., «El régimen jurídico de los prestadores de servicios de la sociedad de la información», en R. Mateu de Ros y M. López-Monís Gallego, M. (coordinadores) Derecho de Internet (La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico), Navarra, Aranzadi, 2003.

YESIL, Magdalena, *Creating the virtual store: taking your web site from browsing to buying*. John Wiley & Sons INC, 1996.