NEWSLETTER DE IP-IT – Septiembre 2017

CONTENIDOS

1. Anteproyecto de Ley Orgánica de protección de datos de carácter personal.

El pasado mes de julio se dio a conocer el Anteproyecto de Ley Orgánica de Protección de Datos, que ha de derogar la vigente normativa nacional sobre esta materia al tiempo que adaptar la legislación española a las disposiciones contenidas en el Reglamento comunitario de 2016 (Reglamento (UE) 2016/679, del Parlamento Europeo y el Consejo, de 27 de abril de 2016) antes de su efectiva aplicación fijada para el próximo 25 de mayo de 2018, que es la fecha que precisamente fija el Anteproyecto como la de entrada en vigor de la norma nacional.

A modo enunciativo y no exhaustivo, destacamos algunos aspectos relevantes del precitado Anteproyecto:

- Datos de fallecidos: se regula por primera vez los derechos de acceso, rectificación o supresión en relación a este tipo de datos.
- Consentimiento (como principio legitimador del tratamiento de datos): conforme al Reglamento comunitario, se exige que se trate de una declaración o de una clara acción afirmativa del afectado, excluyendo de tal modo el consentimiento tácito.
- Minoría de edad: se fija en 13 años, frente a los 14 actuales.
- Tratamientos de datos basados en una ley e interés legítimo: diferenciándose entre el tratamiento exigido por una previsión legal o en el interés legítimo, señalando que nada obsta a la concurrencia de un interés legítimo aun cuando no exista una previsión legal específica.
- Categorías especiales de datos: precisa que, con relación a determinados datos considerados como sensibles (no todos), se prevé que no bastará con el consentimiento del afectado para levantar la prohibición para realizar aquellos tratamientos de datos cuya finalidad principal sea identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.
- Datos de contacto de personas físicas que prestan servicios en una persona jurídica: considera el texto la concurrencia de un interés legítimo en la medida en que se respete el principio de minimización (datos imprescindibles) y que la finalidad de su tratamiento sea la gestión de las relaciones B2B.
- Datos hechos manifiestamente públicos por el afectado: esta importante novedad se refiere a la licitud del tratamiento de este tipo de datos (excluidos datos de menores de edad o personas con discapacidad) siempre que se respeten determinadas condiciones (información y garantía del ejercicio de los derechos del afectado).
- Ficheros comunes: el texto retoma el régimen aplicable a los denominados “ficheros comunes” sobre solvencia patrimonial y crédito, aunque con algunas particularidades (p.e: bloqueo del tratamiento mientras se informa al afectado de su inclusión en tal fichero o cuantía mínima para la inclusión en dichos ficheros). Del mismo modo se retoma la regulación existente en nuestra vigente normativa sobre los sistemas de exclusión publicitaria (“Listas Robinson”), exigiendo obligaciones no desconocidas hasta la fecha como la de consulta de estos ficheros comunes.
- Vídeo vigilancia: el texto dedica un artículo sobre esta actividad, recogiendo los criterios de la AEPD y la jurisdicción revisora en los últimos años. Así, por ejemplo, se refiere a la prohibición de captar imágenes en la vía pública salvo que resulte imprescindible para preservar la seguridad de las personas y bienes así como sus instalaciones.

- *Whistleblowing*: se regula legislativamente por primera vez, siendo destacable que, al contrario del criterio mantenido hasta la fecha, se permiten denuncias anónimas.
- Tratamiento de datos en operaciones mercantiles: el precepto regula los supuestos de hecho hasta ahora contemplados en el artículo 19 del actual reglamento de desarrollo de la LOPD pero con novedades importantes y de calado, por cuanto se refiere a tratamientos "previos" a la operación mercantil de que se trate, refiriéndose igualmente a conceptos como la aportación o transmisión de negocio o rama de actividad empresarial.
- Derechos de las personas: en cuyo título se incluyen las previsiones sobre transparencia e información con una referencia expresa al suministro de la misma por "capas" en caso de obtención de datos en el marco de la prestación de servicios de la información o a través de redes de comunicaciones electrónicas; así como previsiones sobre el ejercicio de los derechos de acceso, rectificación, supresión, oposición, portabilidad o limitación al tratamiento. Destaca en este título el régimen sobre la obligación de bloqueo de datos que no consta en el Reglamento Europeo.
- Medidas de responsabilidad proactiva: en las que se regula, entre otras circunstancias, la evaluación de impacto, incluyendo un listado no exhaustivo de supuestos donde se aprecian mayores riesgos en el tratamiento de datos (p.e: crear o utilizar perfiles personales, mediante el análisis o la predicción de aspectos referidos a su situación económica, salud, preferencias o intereses personales; tratamiento de datos especialmente protegidos; cuanto el tratamiento pueda generar situaciones de discriminación o daño a la reputación, etc.).
- Delegado de Protección de Datos: destaca de su regulación el listado de supuestos en los que se considera obligatoria la designación del DPO, que incluye ficheros comunes, centros docentes, centros sanitarios, prestadores de servicios de la sociedad de la información, sector bancario y de seguros, seguridad privada; distribuidores y comercializadores de energía o gas, entidades que exploten redes y presten servicios de comunicaciones electrónicas.
- Códigos de conducta y esquemas de certificación: destacando la previsión en la que se confiere a la ENAC (Entidad Nacional de Acreditación) la función de acreditación y certificación prevista por el Reglamento para organismos de certificación en materia de protección de datos.
- Agencia Española de Protección de Datos: se regula la naturaleza, régimen jurídico y funciones y competencias del regulador, incluyendo la novedad relativa a los denominados "planes de auditoría preventiva" que parece vendrían a ser las actuales "inspecciones sectoriales" con el matiz de que se indica que las directrices que resulten de dichos planes serán obligatorias para el sector objeto de la misma. Se regulan igualmente disposiciones específicas para los procedimientos tramitados por la autoridad.
- Régimen sancionador: el régimen cualifica las infracciones tipificadas en el Reglamento comunitario como muy graves, graves y leves a efectos de los plazos de prescripción y se refiere a los criterios de graduación del texto europeo, añadiendo otros supuestos que funcionarían como atenuante o agravantes.

Más información en el siguiente **enlace**.

• • •

2. Grupo de Trabajo del Artículo 29: "*Guidelines on data protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purpose of Regulation 2016/679*".

El Reglamento Europeo de Protección de Datos, aplicable a partir del 25 de mayo de 2018, introduce en su artículo 35 el concepto de Evaluación del impacto de la protección de datos (por sus siglas en inglés, DPIA). La DPIA es el proceso diseñado para describir el tratamiento de datos, determinar su necesidad y ayudar a la gestión de los riesgos para los derechos y libertades de las personas físicas resultantes de dicho tratamiento.

Como destaca el GT29, la referencia a los derechos y libertades de los sujetos está totalmente vinculada con el derecho a la privacidad, pero también incluye otros derechos fundamentales como son la libertad de expresión, la libertad de pensamiento, la libertad de movimiento, la prohibición de discriminación, el derecho a la libertad, conciencia y religión.

La DPIA es una herramienta útil para los responsables del tratamiento ya que no sólo describe los requisitos del Reglamento, sino que también sirve para demostrar que las medidas adoptadas para asegurar el correcto cumplimiento son las adecuadas. En otras palabras, una DPIA es un proceso o herramienta de gestión de riesgos para dar cumplimiento a la norma y acreditación del principio de *accountability*.

Directrices

Se establece que no es obligatorio realizar una DPIA en todas las operaciones de tratamiento de datos, sino cuando sea probable que un tipo de tratamiento "entrañe un alto riesgo para los derechos y libertades de las personas física" (Artículo 35). Las Directrices tienen como objetivo aclarar el concepto de DPIA así como fijar una lista de operaciones que necesitan DPIA a nivel europeo, una lista de las operaciones que no necesitan DPIA y los criterios comunes para realizar una DPIA.

No hay una lista tasada de tratamientos que requieran DPIA por lo que el Reglamento aporta una serie de criterios que deben ser considerados:

- Evaluación o calificación: especialmente datos sobre aspectos relativos a situación económica, salud, referencias personales o intereses y movimientos (Considerandos 71 al 91).
- Decisiones automatizadas respecto de efectos legales o similares (Artículo 35.3.a).
- Supervisión sistemática (Artículo 35.3.c). Este tipo de supervisión se utiliza como criterio ya que es posible que se obtengan datos personales en circunstancias en que los sujetos no son conscientes de ello o no conocen la forma en que esos datos serán utilizados.
- Datos sensibles: esto incluye las categorías del Artículo 9 además de las relativas a las condenas penales u ofensas.
- Tratamiento de datos a gran escala: el Reglamento no define "gran escala", sin embargo el Considerando 91 establece algunas pautas. El Grupo de Trabajo 29 (en los sucesivo, GT29)recomienda que los siguientes factores sean tenidos en cuenta para determinar si el tratamiento es de "gran escala":

1. Número de datos, tanto cantidad como proporción respecto de población relevante.
2. Volumen de datos o el rango de datos diferentes en proceso de tratamiento.
3. La duración o permanencia de los datos.
4. El ámbito geográfico del tratamiento.

- Conjunto de datos emparejados o combinados.
- Datos relativos a sujetos vulnerables (Considerando 75).
- Usos innovadores o en aplicación de herramientas tecnológicas u organizacionales.
- Transferencia de datos que circulan a través de las fronteras hacia el exterior de la UE (Considerando 116).
- En los casos en que el propio tratamiento prevenga a los sujetos de ejercitar un derecho o de utilizar un servicio o contrato (Artículo 22 y Considerando 91).

Por regla general, conforme al criterio del GT29, las operaciones de tratamiento que cumplan al menos **dos requisitos** requieren la realización de una DPIA. Sin embargo, en algunos casos en que únicamente cumpla un requisito, también será necesaria. En los casos en que la conveniencia de la DPIA sea dudosa, el GT29 recomienda la realización ya que es una herramienta útil para los responsables del tratamiento.

Adicionalmente, el GT29 recomienda llevar a cabo DPIA en operaciones que ya estaban en marcha antes de la fecha de aplicación del Reglamento.

Como muestra de buena voluntad, la DPIA debe llevarse a cabo continuamente durante los procesos de tratamiento ya que los riesgos pueden variar como consecuencia de un cambio en los componentes del tratamiento o como consecuencia del contexto en que el tratamiento se realiza. Sin embargo, debe re-evaluarse en 3 años, antes si es posible, dependiendo de la naturaleza del tratamiento.

¿Cómo llevar a cabo una DPIA?

1. La DPIA debe realizarse antes del tratamiento e irse actualizando en paralelo al avance del proyecto, lo que asegura que la protección de los datos y la privacidad se están cumpliendo.
2. El responsable del tratamiento es el responsable de garantizar que la DPIA se está realizando. Esto es así aunque la DPIA la esté llevando a cabo alguien distinto al responsable (tanto fuera como dentro de la organización).
3. Los responsables tienen flexibilidad para definir la estructura de la DPIA; sin embargo, sea cual sea la forma elegida, ésta debe contener una evaluación de los riesgos de forma que los responsables puedan diseñar las medidas adecuadas.
4. A pesar de no constituir un requisito legal, se recomienda la publicación de la DPIA ya que el objetivo es ayudar al responsable a demostrar el cumplimiento de las normas y la transparencia.

Las DPIAs, ya que ayudan a los responsables del tratamiento a implementar sistemas que cumplan con los requisitos recogidos en el Reglamento. Es por esto que además de los procesos que requieren DPIA obligatoriamente, el GT29 recomienda su realización en todo caso.

Más información en el siguiente **enlace**.

3. Grupo de Trabajo del Artículo 29: Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento.

El objetivo de las Directrices es ayudar a determinar e identificar cuál es la autoridad de control principal ("lead supervisory authority") de un tratamiento transfronterizo.

A este respecto, tras fijar el concepto "tratamiento de datos personales fronterizos" por referencia al artículo 4(23) del Reglamento General, el texto analiza en qué situaciones se entiende que un tratamiento "afecta sustancialmente" a interesados de más de un Estado miembro, concluyendo la necesidad de un análisis caso por caso, teniendo en cuenta el contexto del tratamiento; el tipo de datos, el propósito del tratamiento y otros factores relacionados principalmente con los riesgos que conlleva el tratamiento de datos para los afectados.

El texto analiza igualmente que debe entenderse por "autoridad supervisora principal" o "autoridad de control principal", señalando que será la autoridad que tiene la responsabilidad principal en una actividad de tratamiento de datos transfronteriza. A estos efectos, es determinante el lugar en el que está localizado el "principal establecimiento" del responsable del tratamiento. Sin embargo, para poder establecer dónde se encuentra el establecimiento principal, es necesario determinar cuál es la administración central del responsable del tratamiento en la UE. El enfoque de la norma europea es que la administración central en la UE es el lugar en que se toman las decisiones sobre los fines y medios del tratamiento de datos personales. A continuación el texto analiza supuestos en los que coexisten varios "establecimientos principales" en diferentes países; supuestos en los que los establecimientos principales no coinciden con el lugar donde está la administración central del responsable del tratamiento así como los casos de grupos de empresas o las situaciones de corresponsabilidad del tratamiento.

Se analiza igualmente supuestos de casos límites, destacando la afirmación relativa a que el Reglamento General no permite el "*forum shopping*". Las nuevas Directrices hacen referencia a que el "*one-stop-shop system*" afecta igualmente a los encargados del tratamiento, señalando que en caso de dos autoridades de control principales distintas o no coincidentes respecto del responsable y encargado la relevante será la primera, siendo la segunda la "autoridad de control concernida" (o la "*supervisory authoruty concerned*"), que podrá expresar su opinión sobre el modo de abordar un asunto.

Más información en el siguiente **enlace**.

• • •

4. Sentencias del Tribunal Supremo, Sala de lo Social, de 31 de enero y 1 de febrero de 2017, sobre video vigilancia en el centro de trabajo y validez de la prueba de video cámara.

El Tribunal Supremo publicó dos sentencias relacionadas con la instalación de cámaras de video-vigilancia en el centro de trabajo, en particular, en relación con la ubicación de cámaras que obtenían imágenes del TPV, y cuyas imágenes fueron la prueba utilizada para el despido de la reclamante, empleada del responsable del tratamiento de video vigilancia.

El Tribunal Supremo analiza previamente la sentencia aportada de contraste, relacionada con el despido de trabajadores por transgresión de la buena fe contractual, deslealtad y abuso de confianza señalando que en los dos procesos se controvirtió sobre la validez de la prueba de vídeo, dado que las empresas no habían informado a sus empleados de la posibilidad de usarlas por motivos disciplinarios, y pese a la identidad sustancial existente habían recaído resoluciones contrapuestas: la sentencia recurrida consideró nula la prueba de video y no admitió la validez de las grabaciones porque la empresa recurrente no advirtió a sus empleados de la posibilidad de usar las imágenes en su contra por motivos disciplinarios, mientras que la sentencia de contraste había estimado que esa falta de información no anulaba la prueba porque la cámara estaba a la vista enfocando la caja, lo que hacía que conociesen su instalación y utilidad por ser pública y notorio su objetivo y finalidad.

La Sala de lo Social concluye, en sendas resoluciones que; “La aplicación de la anterior doctrina al presente caso obliga a estimar el recurso porque la instalación de cámaras de seguridad era una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros, así como rápida detección de siniestros), idónea para el logro de ese fin (control de cobros y de la caja en el caso concreto) y necesaria y proporcionada al fin perseguido, razón por la que estaba justificada la limitación de los derechos fundamentales en juego, máxime cuando los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo pero que excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc. etc.. Y frente a los defectos informativos que alegan pudieron reclamar a la empresa más información o denunciarla ante la Agencia Española de Protección de Datos, para que la sancionara por las infracciones que hubiese podido cometer”.

Más información en el siguiente **enlace**.

• • •

5. Sentencia del Tribunal Supremo, Sala de lo Civil, de 2 de febrero de 2017, sobre la existencia y requisitos de la marca notoria.

El Tribunal Supremo ha publicado una sentencia en la que analiza la existencia y requisitos de la marca notoria, destacando que:

- Basta que el grado de similitud entre el signo y la maca de renombre tenga como efecto que el público pertinente establezca un vínculo entre ambos. Es decir, la confusión en sentido amplio incluye aquellos supuestos en que se induce a creer que entre la persona que emplea el signo cuestionado y el titular de la marca anterior existe un vínculo económico o jurídico que autoriza su uso.
- Ahora bien, la existencia de dicho vínculo en la mente del público constituye una condición necesaria pero insuficiente ya que para que exista infracción es necesario que mediante la evocación de la marca notoria, el empleo del signo conlleve un aprovechamiento indebido del carácter distintivo de la marca.
- Para evaluar la semejanza entre dos marcas ha de hacerse la comparación en un triple plano: gráfico, fonético y conceptual. Pero los criterios para determinar la semejanza dependen de la estructura del signo.

En este caso, la Audiencia considera que no existe ningún riesgo de confusión, puesto que los signos en conflicto son acusadamente diferentes y sus únicas similitudes son accesorias. El único elemento común que tiene las marcas en conflicto es la mención al término 24 horas, pero no coinciden ni los colores ni elementos gráficos muy relevantes.

Más información en el siguiente **enlace**.

. . .

6. Sentencia del Tribunal de Justicia de la UE (Gran Sala), de 21 diciembre de 2016, sobre el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas.

El Tribunal de Justicia de la UE (TJUE) publicó una sentencia en la que analiza las peticiones de decisión prejudicial que tienen por objeto la interpretación del artículo 15 de 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.

Estas peticiones han sido presentadas en el marco de dos litigios: el primero entre Tele2 Sverige AB y la Post-och telestyrelsen, en relación con el requerimiento dirigido por esta última a Tele2 Sverige para que procediera a la conservación de los datos de tráfico y de localización de sus abonados y usuarios registrados. El segundo, entre los Sres. Tom Watson, Peter Brice y Geoffrey Lewis, por un lado, y el *Secretary of State for the Home Department* por otro, en relación con la conformidad con el Derecho de la Unión del artículo 1 de la Ley 2014 sobre conservación de datos y facultades de investigación.

La Sentencia concluye que el artículo 15.1 de la precitada Directiva debe interpretarse en el sentido de que se opone una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica.

En el mismo sentido, debe interpretarse (oposición) una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o a una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión.

Más información en el siguiente **enlace**.

• • •

7. Sentencia de la Audiencia Provincial de Castellón de la Plana de 10 de enero de 2017 (SAP CS 1/2017). Obtención de IMEI e IMSI por las Fuerzas y Cuerpos de Seguridad del Estado.

Destacamos esta resolución judicial en la que en su Fundamento Jurídico Primero, trata sobre la obtención de los números IMEI en el contexto de una investigación judicial. Destaca el Tribunal que no sólo las Fuerzas y Cuerpos de Seguridad del Estado están habilitados ex artículo 22 de la LOPD para su obtención sin necesidad de autorización judicial sino que, asimismo, ni dichos datos "per se" pueden ser considerados como datos sensibles ni se trata de datos integrables en el concepto de comunicación (en el contexto del derecho al secreto de las comunicaciones).

Concluye la sentencia, tras referirse a la modificación operada en la LECr en 2015, que "… es decir, no solamente no se necesita autorización judicial para obtener el IMSI o IMEI, sino, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones".

Más información en el siguiente **enlace**.

• • •

8. Sentencia del Tribunal Supremo, Sala de lo Civil, de 1 de Junio de 2017, sobre vulneración de los derechos fundamentales a la intimidad y a la protección de datos.

Una atleta participante en competiciones internacionales del más alto nivel demandó a la Real Federación Española de Atletismo y a la Asociación Internacional de Federaciones de Atletismo solicitando se declarase la intromisión ilegítima por parte de ambas en su derecho a la intimidad mediante la obtención de análisis de sangre y la conservación de dichos datos.

El Juzgado de Primera Instancia y la Audiencia Provincial desestimaron las pretensiones del reclamante afirmando que: (i) el control de dopaje está previsto para las federaciones y las instituciones internacionales tanto en competiciones como fuera de ellas a deportistas con licencia española, y un deportista, al obtener la licencia federativa, asume las normas de competición y antidopaje tanto de su federación de origen como de la competición internacional; y (ii) la toma y conservación de muestras corporales son necesarias para proteger la integridad corporal de los deportistas en orden a detectar el uso de sustancias o métodos prohibidos que pudieran afectar a la salud y la limpieza en la competición deportiva.

La demandante interpuso recurso de casación basado en:

1. La finalidad de luchar contra el dopaje no ampara cualquier medida de investigación, en concreto "el pasaporte biológico"; este motivo fue desestimado pues el término "pasaporte sanguíneo" hace referencia a la realización de controles en los que se obtuvieron muestras de sangre de la demandante y se conservaron durante cierto tiempo los datos obtenidos del análisis de tales muestras. Señala la resolución judicial que lo relevante no es lo relativo al pasaporte en sí, sino a los análisis de sangre y la conservación de los datos; además del consentimiento de la propia demandante.
2. Doctrina del Tribunal Constitucional sobre la ponderación en caso de conflicto entre derechos fundamentales, alegando que la ponderación solo procede cuando se enfrentan dos derechos o bienes constitucionalmente protegidos, y la limpieza en la competición no lo es. El Alto Tribunal desestima el motivo señalando que la protección de la salud y de la limpieza en el deporte son bienes jurídicos de reconocimiento constitucional. La salud que es objeto de protección es no solo la del deportista sometido al control, sino en general la de todos los que participan en las competiciones deportivas y podrían verse inclinados a incurrir en prácticas de dopaje para poder competir en igualdad de condiciones si no existieran los controles.
3. Infracción del principio de proporcionalidad ya que existen medidas más moderadas contra el dopaje como son los análisis de orina; el TS desestima también este motivo indicando que las extracciones y los análisis de sangre y la conservación de los datos obtenidos son el método adecuado para el control del dopaje. No puede limitarse al que tenga por objeto la detección de sustancias prohibidas (análisis de orina) sino que también abarca la detección de métodos prohibidos, como es el caso del dopaje sanguíneo.

Más información en el siguiente **enlace**.

• • •

9. Sentencia de la Audiencia Nacional, Sala de lo Contencioso, de 7 de abril de 2017, sobre los requisitos necesarios para la cesión de datos personales a terceros.

La Sala de lo Contencioso de la Audiencia Nacional publicó una sentencia en la que, con ocasión de una eventual cesión de datos entre dos entidades pertenecientes a un importante grupo del sector *retail*, revisa el alcance, naturaleza y contenido de la institución de la cesión de datos. En suma, destaca que los requisitos de la cesión son: (I) el consentimiento previo del afectado; (ii) la necesaria relación de la cesión con el cumplimiento de los fines del cedente, y (iii) la necesaria relación de la cesión relacionada con los fines del cesionario.

En el caso analizado, considera la Audiencia que la finalidad prevista para la cesión entre una entidad del grupo (entidad financiera) a otra (aseguradora), esto es, la de "facilitar las operaciones comerciales" no habilitaba a la cesionaria para la utilización de los datos para realizar acciones comerciales. Por consiguiente, concluye que las acciones publicitarias llevadas a cabo por tal cesionaria no contaban con el consentimiento expreso o tácito del denunciante, de lo que resulta la infracción del artículo 11 de la LOPD.

Más información en el siguiente **enlace**.

. . .

10. Sentencia de la Audiencia Nacional, Sala de lo Contencioso, de 28 de marzo de 2017. Requerimiento de pago previo a la inclusión en un fichero de información sobre solvencia patrimonial y crédito.

La Sentencia se refiere a un supuesto infractor de la normativa sobre protección de datos por la indebida inclusión de datos en un fichero sobre solvencia patrimonial y crédito como consecuencia de la ausencia (o no acreditación de su realización) del preceptivo requerimiento previo de pago.

Resulta de sumo interés el análisis que se realiza sobre el carácter de prueba indiciaria de los correos electrónicos y mensajes SMS que envió la entidad recurrente/acreedora requiriendo el pago de la deuda, que constituye uno de los requisitos necesarios para la posterior inclusión de la deuda en los ficheros comunes. Sobre los correos electrónicos en particular, la Audiencia Nacional señala que "argumentando en relación con los correos electrónicos aportados por la actora y enviados a su destinatario, que el envío efectivo de un correo electrónico por parte del servidor de origen no implica su recepción por el servidor de correo destinatario, porque la confirmación de la recepción de los correos electrónicos depende del funcionamiento del resto de los servidores de correo intervinientes en la comunicación y muy especialmente del servidor de correo de la cuenta destinataria".

Con relación a los SMS enviados a la denunciante, señala que, como se dice en la sentencia de la Audiencia Nacional de 14 de noviembre de 2013 "la mera constancia en los registros informáticos de la empresa, del envío de los mensajes SMS, no resulta prueba suficiente de efectivo envío. Y en todo caso tampoco acredita ni la efectiva recepción del envío ni menos aún de su apertura por la persona del destinatario".

De este modo, el órgano judicial no considera dichos envíos siquiera como una prueba indiciaria pese a circunstancias como (i) que los datos del denunciante relativos al correo electrónico o número de teléfono utilizados para dichos envíos los había aportado el mismo; o (ii) que dicho denunciante había procedido al pago de la deuda siguiendo el procedimiento indicado en alguno de dichos envíos.

Con todo, aun admitiendo que el acreedor puede utilizar cualquier medio para la realización del requerimiento de pago, concluye que en este caso no consta acreditada la recepción de los mensajes ni por tanto la realización del mismo.

Más información en el siguiente **enlace**.

• • •

11. Sentencia del Tribunal Supremo, Sala de lo Civil, de 26 de abril de 2017, sobre los criterios de valoración del daño moral en supuestos contra el derecho al honor por inclusión en ficheros de morosos.

El Tribunal Supremo ha dictado una sentencia en la que viene a exponer los criterios que deben ser considerados para la fijación del importe o suma de las indemnizaciones derivadas de la infracción del derecho al honor (resarcimiento de los daños morales) que traen causa en la indebida incorporación de datos personales en un fichero de información sobre solvencia patrimonial y crédito.

Al efecto, señala que en el análisis que debe realizarse en cada caso concreto y partiendo del contenido del artículo 9.3 de la Ley Orgánica 1/82 (presunción *iuris et de iure* de existencia de perjuicio si se acredita la intromisión ilegítima) las cuestiones relevantes serían: (i) inadmisibilidad de indemnizaciones meramente simbólicas; (ii) divulgación de la información errónea (esto es, conocimiento de terceros con acceso al fichero común); (iii) quebranto o angustia por las gestiones realizadas por el perjudicado para lograr la rectificación o cancelación del dato incorrecto; (iv) irrelevancia de la escasa cuantía de la suma para valorar la importancia del daño moral o (v) tiempo en el que la deuda estuvo incluida en tal fichero común.

Más información en el siguiente **enlace**.

• • •

12. Sentencia de la Audiencia Nacional, Sala de lo Contencioso, de 20 de abril de 2017. Caducidad del expediente.

La Audiencia Nacional ha publicado una sentencia en relación con el recurso interpuesto contra la resolución dictada por el Director General de la AEPD por la que impone a la entidad LA MANGA CLUB, S.L, una sanción por la comisión de una infracción del artículo 4.1 tipificada como grave. La sentencia estima las alegaciones formuladas por el recurrente relativas a la caducidad del expediente sancionador, toda vez que entre la fecha de incoación del expediente sancionador y aquella en la que se notifica la resolución del expediente, habían transcurrido más de seis meses (art. 48.3 de la LOPD).

Más información en el siguiente **enlace**.

• • •

13. Sentencia del Tribunal Supremo, Sala de lo Contencioso, de 21 de marzo de 2017, sobre la inviolabilidad del domicilio de la persona jurídica y el secreto de las comunicaciones.

El Tribunal Supremo ha publicado una sentencia en relación con el recurso de casación contra la sentencia de la Audiencia nacional en un procedimiento relativo a la actuación inspectora de la CNMC.

Recogiendo la Jurisprudencia Constitucional ha declarado que el núcleo esencial del domicilio constitucionalmente protegido es el domicilio en cuanto a morada de las personas físicas y reducto de su intimidad personal y familiar. Respecto del domicilio de las personas jurídicas, señala que. si bien son titulares del derecho que reconoce el art. 18.2, gozan de una intensidad menor de protección.

En este sentido, declara que no todo domicilio registral o mercantil alcanza la consideración de domicilio constitucionalmente protegido, siendo necesario que, para gozar de tal protección, estemos ante:

- Espacios físicos que son indispensables para desarrollar la actividad sin intromisiones ajenas, por constituir el centro de dirección de la sociedad o de un establecimiento dependiente.
- Espacios destinados a la custodia de documentos u otros soportes de la vida diaria de la sociedad o de un establecimiento que quedan reservados al conocimiento de terceros.

A *sensu contrario*, no son objeto de tal protección los establecimientos abiertos al público o que lleven a cabo una actividad laboral o comercial por cuenta de una sociedad mercantil que no está vinculada con la dirección de la sociedad o de un establecimiento, ni sirva a la custodia de su documentación.

Más información en el siguiente **enlace**.

• • •

14. Sentencia del Tribunal Supremo, Sala de lo Civil, de 15 de febrero de 2017, sobre el derecho a la propia imagen y a la intimidad personal y familiar. Publicación en un periódico de una fotografía obtenida de Facebook.

El Tribunal Supremo ha publicado una sentencia en relación con la edición del diario "La Opinión – El Correo de Zamora" que publicó un reportaje sobre un suceso en el que el demandante fue herido por su hermano, quien le disparó y después se suicidó. En el reportaje, además, se incorporó una fotografía del demandante obtenida de su perfil de Facebook.

En relación a la tradicional controversia sobre la prevalencia de la libertad de información frente al derecho a la intimidad personal y familiar la Sala, tras poner de manifiesto la dificultad de establecer pautas generales que sirvan para todos los casos considerada que en el caso analizado concurren circunstancias que determinan la prevalencia de la libertad de información, ya que la intromisión en la vida personal no puede considerarse grave o intensa; los hechos son expuestos sin extralimitación morbosa (sino según los cánones de la crónica de sucesos) y no se desvelan hechos íntimos sin relación con lo sucedido. Indica además, que se trata de un ámbito geográfico reducido (Zamora), de un periódico provincial y por tanto la información es especialmente relevante y acomodada a sus usos sociales.

Por otro lado, el Tribunal sí considero la utilización de la fotografía extraída de Facebook como una intromisión en el derecho a la propia imagen ya que, tras declarar que tal derecho es distinto y autónomo de los derechos a la intimidad personal y familiar, considera conforme a otros precedentes que cita, que tener una cuenta abierta y accesible al público no implica un consentimiento expreso que autorice a un tercero a publicar las imágenes allí contenidas. En particular, señala que la publicación de la imagen en dicha red social, "no autoriza a un tercero a reproducirla en un medio de comunicación sin el consentimiento del titular, porque tal actuación no puede considerarse una consecuencia natural del carácter accesible de los datos e imágenes de un perfil público de una red social en Internet"

Más información en el siguiente **enlace**.

. . .

15. El Tribunal Supremo avala que las empresas comuniquen las nóminas en soporte informático y no en papel.

El Tribunal Supremo considera ajustado a Derecho que las empresas comuniquen las nóminas del mes a los trabajadores en soporte informático y no en soporte papel.

Se modifica así la doctrina al respecto plasmada en la sentencia de 22 de diciembre de 2011, referida a la empresa Air Europa. La razón del cambio de criterio radica en el tiempo transcurrido y en la generalización de la utilización del soporte informático en lugar del soporte papel.

La sentencia del TS rechaza el recurso de USO de Asturias que interesaba que se declarase nula la decisión de Transportes Unidos de Asturias S.L de comunicar la nómina a través de soporte informático.

El alto tribunal indica que se exige la entrega al trabajador de un recibo individual justificativo del pago del salario, pero no se establece el soporte. Podría parecer que la entrega se exige en papel, a tenor del artículo 2 de la Orden de 27 de diciembre de 1994; sin embargo, tal apariencia queda desvirtuada por el apartado 2 del precepto, cuando señala que "Cuando el abono se realice mediante transferencia bancaria, el empresario entregará al trabajador el duplicado del recibo sin recabar su firma, que se entenderá sustituida por el comprobante del abono expedido por la entidad bancaria".

En definitiva, la operación, que antes consistía en abrir el buzón mediante llave, ahora se realiza introduciendo en el terminal el número de DNI y la clave, lo que no supone perjuicio al trabajador.

• • •

16. Sentencia del TJUE, de 4 de mayo de 2017, sobre la solicitud de comunicación de datos personales para ejercer un derecho en un procedimiento judicial.

El Tribunal ha publicado una sentencia en relación con un accidente de tráfico que se produjo en Riga, se incoó un procedimiento administrativo sancionador y se levantó el atestado correspondiente.

La empresa explotadora del servicio de trolebús dañado se dirigió a la Policía Nacional, solicitando los datos de la persona que hubiera sido sancionada en vía administrativa. La Policía comunico el nombre y apellidos del sujeto alegando que la documentación obrante en un expediente sancionador solo la pueden recibir quienes son parte del mismo. El propietario impugno la resolución ya que se negaban a revelar el número de identificación y el domicilio del individuo implicado en el accidente.

El Tribunal plantea una cuestión prejudicial: ¿La frase "es necesario para la satisfacción del interés legítimo perseguido por […] el tercero o terceros a los que se comuniquen los datos", debe interpretarse como que la Policía deba revelar los datos de carácter personal necesarios para interponer recurso?

El Tribunal de Justicia ha declarado que el artículo 7, letra f) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que no obliga a comunicar datos personales a un tercero para que éste pueda interponer una demanda indemnizatoria en vía civil por los daños causados. Sin embargo, el artículo 7, letra f), de esta Directiva, **no obsta a que, al amparo del Derecho Nacional, se produzca tal comunicación**.

Más información en el siguiente **enlace**.

• • •

17. Sentencia del Tribunal de Justicia de la Unión Europea, de 9 de marzo de 2017, sobre datos personales sujetos a publicidad en el registro de sociedades y su acceso o posible cancelación o supresión transcurrido un plazo.

El Sr. Manni, administrador único de una sociedad de italiana Construzioni Srl, a la que se adjudicó un contrato para la construcción de un complejo turístico; demandó ante los tribunales a la Cámara de Comercio de Lecce, alegando que los inmuebles del complejo no se vendían porque en el registro de sociedades constaba que él había sido administrador único y liquidador de la sociedad italiana Salentina, declarada en concurso de acreedores.

Mediante sentencia, el Tribunal de Lecce, estimó sus pretensiones en base a que los asientos que vinculan el nombre de una persona física a una fase crítica de la vida de la empresa (concurso de acreedores) no pueden ser indefinidos.

El Tribunal Supremo de casación, que conoce del recurso, decidió suspender el procedimiento y plantear al Tribunal de Justicia la siguiente cuestión: ¿permite el artículo 3 de la […] Directiva 68/151 […] que, como excepción a que los datos publicados en el registro de sociedades tengan vigencia ilimitada y puedan ser consultados por destinatarios indeterminados, tales datos ya no sean "públicos" en ese doble sentido, sino que sólo estén disponibles durante un periodo limitado o para destinatarios concretos en virtud de una apreciación caso por caso del responsable de esos datos?

El Tribunal afirma en primer lugar que los datos del recurrente son datos de carácter personal no obstante se trate de información que se integra en el contexto de una actividad profesional. Del mismo modo, señala que la incorporación y conservación en un registro así como su puesta a disposición de terceros, supone asimismo un "tratamiento".

Por otro lado, atiende a los argumentos del Abogado General al afirmar que este tratamiento tiene su legitimidad en varios supuestos de la Directiva, en concreto, el cumplimiento de una obligación legal; el ejercicio de una autoridad pública o de una misión de un interés público y, finalmente, la realización de un interés legítimo.

Prosigue señalando que, para analizar si procede satisfacer el derecho al bloqueo o supresión de esta información, es relevante acudir a la finalidad de la inscripción registral, destacando en este sentido que, en el caso que nos ocupa, la finalidad principal – entre otras- es dar publicidad a terceros sobre actos esenciales de las sociedades y, en particular, sobre las personas que tienen el poder para obligarla.

En relación al plazo de conservación, se refiere a la posible subsistencia de derechos y obligaciones tras la extinción de la sociedad así como a los plazos de prescripción aplicables en los distintos Estados Miembros, destacando que la Directiva no señala plazos concretos.

El Tribunal explica que aunque la necesidad de proteger intereses de terceros y de seguridad jurídica, pueden existir situaciones particulares en los que se observen motivos preponderantes que permitan la cancelación de los datos, si bien destaca que el motivo aportado por el recurrente (imposibilidad actual de vender inmuebles) no parece suficiente. Sin perjuicio de lo anterior, el Tribunal concluye que en el estado actual del Derecho de la Unión, **incumbe a los Estados miembros determinar** si las personas físicas pueden solicitar a la autoridad responsable de la llevanza del registro central, del registro mercantil o del registro de sociedades, respectivamente, que compruebe si está excepcionalmente justificado, limitar, al expirar un plazo suficientemente largo tras la disolución de la empresa de que se trate, el acceso a los datos personales que les conciernen, inscritos en dicho registro, a los terceros que justifiquen un interés específico en la consulta.

Más información en el siguiente **enlace**.

• • •

Si desea más información sobre estos temas o cualquier otro asunto relacionado, puede ponerse en contacto con el equipo de profesionales del área de IP-IT de BROSETA.

Contactos del área de IP-IT de BROSETA

Miguel Geijo
Socio. Director del Área
mgeijo@broseta.com
Tel.: +34 91 432 31 44

Carolina Vivó
Abogada
cvivo@broseta.com
Tel.: +34 91 432 31 44

Alicia Coloma
Abogada
acoloma@broseta.com
Tel.: +34 91 432 31 44

BROSETA
Goya, 29. Madrid, 28001 / Pascual y Genís, 5. Valencia, 46002
Tel. + 34 91 432 31 44 / Tel. +34 96 392 10 06
info@broseta.com / www.broseta.com