Día Europeo de la Protección de Datos

28 enero

2019

ECIJA

Día Europeo de la Protección de Datos - Newsletter ECIJA

Desde el **Área de Privacidad y Protección de Datos de ECIJA** hemos analizado en la presente Newsletter, temas de absoluta actualidad empresarial y jurídica, como el ejercicio de derechos por las personas (tanto el derecho de supresión como los sistemas de exclusión publicitaria) y las implicaciones que tienen para responsables del tratamiento, encargados y solicitantes, las relaciones entre tecnología y derecho (analizando cuestiones como **blockchain, cookies** o la utilización **algoritmos**), así como el estudio con la mirada puesta en el futuro sobre la normativa y su aplicación. Igualmente, abordamos cuestiones relativas a **tratamientos concretos de datos**, tales como el impacto en el mundo de la **moda, la videovigilancia, los datos biométricos, la segmentación y profiling, su impacto con PSD2**, así como la necesaria evolución del deber de información para que todos los aspectos enunciados, puedan realizarse de forma legítima, mitigando riesgos y permitiendo la innovación en la era digital.

Día Europeo de la Protección de Datos - Newsletter ECIJA

Área de Privacidad y Protección de Datos de ECIJA

www.ecija.com

Día Europeo de la Protección de Datos - Newsletter ECIJA

El ejercicio del derecho de supresión en la LOPDGDD

María Manso y Mar Ibáñez, abogadas de ECIJA

El **ejercicio del derecho de supresión** no requiere necesariamente una acción activa por parte del interesado para que se supriman los datos. Es decir, debido al principio de calidad de los datos que se reconoce tanto en la derogada Ley Orgánica 15/1999, así como en la normativa vigente en materia de Protección de Datos, éstos deberán ser suprimidos cuando ya no sean necesarios. Igualmente, es obligatorio suprimir los datos cuando se hayan recogido o tratados de forma ilícita. Pero la cuestión es: **¿cuándo no son necesarios para la compañía?** Dicho momento llega cuando ya no sean necesarios para los fines para los que fueron recogidos o tratados por parte de la propia entidad.

Una cuestión frecuente entre las compañías es **cómo actuar en caso de recibir por parte de un interesado la petición de suprimir sus datos**, siendo esta acción un derecho reconocido al mismo que puede ejercer en cualquier momento comunicando esta decisión a la propia entidad que esté tratando sus datos.

Efectivamente, el derecho de supresión es un derecho reconocido por el artículo 17 del 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 (RGPD), pero, ¿qué ocurre cuando la compañía presenta la necesidad de conservar los datos?

La supresión no siempre se puede llevar a cabo **de forma inmediata y total** en el momento de la solicitud del interesado, puesto que la obligación de supresión debe entenderse conjuntamente con el interés o necesidad de la compañía de conservar esta información para demostrar el cumplimiento de sus obligaciones legales y responsabilidad en el cumplimiento de las finalidades para las que los datos fueron recabados.

En este sentido, en ocasiones, la supresión total de los datos puede causar un perjuicio en los intereses legítimos de la compañía que los trata; no obstante, tendrá que atenderse de forma obligatoria a este derecho y **realizar acciones proactivas** que, sin llegar a eliminar los datos de forma definitiva, se consiga un bloqueo de los mismos de forma que los datos no sean gestionados ni tratados y se conserven únicamente a disposición de administraciones públicas, jueces y tribunales, para la atención de posibles responsabilidades derivadas del tratamiento, y únicamente durante el plazo de prescripción de éstas. Cuando el plazo se cumpla, se deberá proceder a la supresión definitiva de los datos.

El bloqueo de los datos implica su conservación, pero permitiendo el acceso a los mismos únicamente a determinadas personas ante casos de acciones, reclamaciones o requerimientos administrativos o de carácter judicial. Durante el proceso de bloqueo de los datos, se debe impedir el tratamiento de los mismos. En este sentido, sería coherente utilizar un **sistema de cifrado de los datos bloqueados,** que garantice su acceso únicamente por personas designadas y en casos determinados.

El plazo de conservación de los datos debidamente bloqueados varía según los plazos de prescripción definidos por las diversas normativas que pudiesen resultar de aplicación al tratamiento de los datos del interesado, pudiendo darse el caso de que apliquen dos o más plazos y no se proceda a la supresión de los mismos hasta que no transcurra el plazo más amplio.

Por su parte, una vez transcurrido el plazo de conservación, la supresión dará lugar a la destrucción definitiva de los datos, de modo que se garantice que la información no puede ser recuperada, bajo ningún concepto, alcanzando la totalidad de las bases de datos, archivos y copias de seguridad, ello con independencia

de que los datos se encuentren en papel, en un software almacenado en recursos corporativos o en un SaaS, en dispositivos de almacenamiento externo o en los propios equipos de la Compañía. Todo ello, con independencia de que la Compañía guarde la evidencia del borrado de los registros.

En definitiva, en ocasiones, el derecho de supresión o, también conocido como **"derecho al olvido"** de los interesados, no puede hacerse efectivo de manera inmediata y total por parte de las compañías, por lo que, en tal caso, las mismas deberán proceder al bloqueo de los datos garantizando que los mismos no serán tratados salvo que se deban poner a disposición de administraciones públicas, jueces y tribunales o, en cualquier caso, para la atención de posibles responsabilidades derivadas del tratamiento.

Los sistemas de exclusión publicitaria: novedades introducidas por la LOPDGDD

Daniela Vidal, abogada de ECIJA

Con ocasión del Día Europeo de la Protección de Datos nos vemos obligados a reflexionar si las novedades introducidas por el legislador español en la reciente Ley Orgánica de Protección de Datos de Carácter Personal y de Garantías de Derechos Digitales (en adelante, "LOPDGDD") en relación con la obligación de consultar e informar sobre las listas de exclusión publicitaria es acorde con el espíritu del 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 y por el que se deroga la Directiva 95/46/CE (en adelante, "Reglamento General de Protección de Datos", o "RGPD").

¿En qué consisten estas dos novedades?

Por un lado, en la obligación de que toda empresa deba consultar las listas de exclusión publicitaria antes de realizar cualquier envío de comunicaciones comerciales, salvo que el interesado hubiese otorgado su consentimiento expreso para recibir las mismas.

Por otra parte, la obligación de las empresas de tener que **informar al interesado**, tras su solicitud de oposición a la recepción de comunicaciones comerciales, de la existencia de tales listas de exclusión publicitaria a las que podrá adherirse de forma gratuita.
Profundizamos un poco sobre esto.

Listas de exclusión publicitaria

Con la legislación anterior, las listas de exclusión publicitaria debían consultarse al **adquirir la base de datos de un tercero**, o al obtener los datos de fuentes accesibles al público, lo cual tenía sentido puesto que jamás se había tenido contacto directo con el titular de los datos, a los efectos de conocer si éste deseaba recibir publicidad.
A partir del 7 de diciembre de 2018, fecha en la que entró en vigor la LOPDGDD, se establece una nueva obligación: consultar las listas de exclusión publicitaria con carácter previo a la realización de mercadotecnia directa, exceptuándose aquellos casos en los que el titular de los datos haya dado su consentimiento, lo que en la práctica se reduce a que figure la casilla de dicha opción marcada.
A contrario sensu de lo que pudiera creerse, en la mayoría de ocasiones la opción no se marca no tanto por

recelo a la publicidad, como por evitar el usuario a toda costa cualquier conducta activa.

Es decir, incluso siendo el interesado cliente, y estando el envío de comunicaciones comerciales legitimado en el interés legítimo (legitimación, que, por otro lado, ha sido avalada tanto por el RGPD como por el Grupo de Trabajo del Artículo 29 en varias de sus Directrices y Opiniones) se deberá consultar las listas de exclusión publicitaria con carácter previo al envío.
Por último, **consultar las listas de exclusión publicitaria lleva aparejado un coste económico**. Esto, a la postre implicará que muchos prefieran subcontratar los servicios a un tercero. Ahora bien, fundamental será regular dicha relación debidamente. Una buena parte de las sanciones impuestas por la Agencia Española de Protección de Datos son consecuencia del incumplimiento de la normativa que regula las comunicaciones comerciales y, muchas de ellas, a causa de una mala gestión en el envío de las comunicaciones comerciales por parte de los terceros contratados.

Deber de información

La segunda obligación consiste en informar acerca de las listas de exclusión publicitaria, cuando cualquier interesado haya manifestado su negativa a recibir comunicaciones comerciales.

¿Es realmente necesario?

Nuestro ordenamiento jurídico ya otorgaba y sigue otorgando un sinfín de obligaciones que las compañías deben poner a disposición de los interesados para que se puedan oponer a recibir comunicaciones comerciales. Se tiene que dar la opción de rechazar la opción al entregar los datos, se debe dar la posibilidad de oponerse a recibir este tipo de comunicaciones, en cada una de las comunicaciones comerciales que se envíen, incluso se tiene que dar la posibilidad al titular de los datos de oponerse a recibir comunicaciones comerciales vía el ejercicio del derecho de oposición.
Es decir, podríamos entender que no era estrictamente necesario incluir este requisito y, sin embargo, la LOPDGDD lo introduce ofreciendo una mayor protección jurídica a los titulares de los datos. Pero, **¿causa esto un perjuicio a las empresas que se dedican al envío de comunicaciones comerciales?** No debemos olvidar que el envío de comunicaciones comerciales es el medio natural para recordar a los consumidores que las empresas y sus productos están ahí fuera, aún con mayor sentido, en un mundo en donde pocos pueden visitar las tiendas físicas, amén de aquellos cuyo negocio se desenvuelve sólo en el mundo virtual. Por no hablar ya del daño que se produce a las PYMES. Porque la mayoría tenemos en la mente a las grandes marcas, pero ¿y los que acaban de empezar o son más pequeños y por ello menos visibles?

En definitiva, está clara cuál es la postura del legislador español hacia el envío de publicidad, pero ¿y el legislador europeo, que opinará al respecto?

El RGPD no se pronuncia sobre esto. Y dado que hoy es el Día Europeo de la Protección de Datos no nos queda más remedio que reflexionar si verdaderamente la finalidad desde Europa era **restringir, aún más, el envío de comunicaciones comerciales.**

La Unión Europea ha querido que se tomase consciencia del uso que las empresas hacen de los datos, que se adoptasen las medidas técnicas y organizativas necesarias para proteger dichos datos de pérdidas y accesos no autorizados, que se le otorgase relevancia a unos datos que en último término pertenecen a su titulares, pero no era intención del legislador que se acabase la economía digital, y las rentas generadas, porque lo cierto es que son un activo fundamental para las organizaciones. El equilibrio entre los derechos de unos y los intereses de otros ha sido siempre la clave de toda esta regulación.
Por suerte estamos los que nos dedicamos a esto, que seguiremos intentando buscar ese equilibrio. Nuestros clientes nos sorprenden día a día con formas innovadoras para seguir avanzando. Tendremos que esperar a ver cómo se desenvuelve todo esto.

Firma líder en asesoramiento en Derecho de Tecnología, Medios y Telecomunicaciones

Aranzazu Monteagudo y Francisco Cantueso, abogados de ECIJA.

Los datos sanitarios se han convertido en el principal activo a proteger por parte de las entidades sanitarias. Su **uso debe ser transparente** de cara al paciente y a garantizar la seguridad de la información.

El creciente desarrollo de las TICs en los últimos años ha afectado a numerosos ámbitos de nuestra vida. Especial relevancia está suponiendo el impacto de las TICs en la medicina, permitiendo un acceso y control del paciente de manera continua, sencilla, inmediata y con calidad en cualquier lugar, contribuyendo de manera exponencial a la universalidad y equidad de los servicios asistenciales, de diagnóstico, monitorización, de formación etc.

Las TICs aplicadas al ámbito sanitario, se han dado a conocer como **E-health**, favoreciendo al avance de la medicina, con un mayor impacto en los servicios sanitarios, disminuyendo los costes de los servicios y su consumo, evitando la duplicidad de pruebas, aumentando la seguridad del paciente y facilitando la coordinación e interoperabilidad entre los diferentes agentes intervinientes.

Actualmente **ya es una realidad la telemedicina y teleasistencia:** dispositivos y aplicaciones móviles al alcance de los pacientes con un solo click, cirugía robótica (como el Da Vinci, Senhance, Flex, el Broca etc.), los robots que "pasan consultan" conectados a un doctor en la otra punta del mundo, que reparten los medicamentos o rellenan jeringuillas con las cantidades exactas, CIM (Cirugía Mínimamente Invasiva o cirugía laparoscópica), dispositivos wearables (monitorización que se integra en la ropa) y sensores intercorporales que permiten medir el estado de salud del paciente en su entorno, analizando por ejemplo la temperatura, el ritmo cardiaco, el ritmo respiratorio etc., o la Inteligencia Ambiental (AmI) que, mediante interfaces intuitivas e inteligentes adheridas a objetos cotidianos y en un entorno, se convierten en sensibles e interactivas siendo capaces de reconocer y dar respuesta al usuario.

Este impulso también se ha debido al aumento de la longevidad y de las patologías crónicas, en cifras de la ONU, se sugiere que la población mayor de 60 años se incrementará para el año 2030 en un 56%, lo que hará necesario contar con servicios de salud más eficientes y baratos, como **herramientas de autodiagnóstico, hospitales automatizados**, en definitiva, un continuo, eficaz, rápido y asequible seguimiento de un paciente.

Y si bien los avances en el campo de la tecnología son cada vez mayores y se despliegan rápidamente, **se plantean problemas en relación a la adaptación de todos estos progresos al marco normativo,** y especialmente a la materia de protección de datos, dado que el uso de toda esta tecnología, no hace otra casa que generar información y datos de pacientes en cantidades ingentes. Datos a los que se accede, que se tratan, se conservan y se transfieren, por una interminable cadena a veces de entidades, cuya integridad y uso para fines diferentes de su aplicación médica, es a día de hoy una realidad que no deja de aumentar. Y lo más complicado, en la mayoría de las ocasiones es que el propio titular (paciente), deja de conocer no solo la ubicación de sus datos, sino también el uso que se les está dando, tratados en ocasiones sin su consentimiento y sin ostentar un verdadero poder de disposición sobre los mismos.

Por medio de la aplicación del 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, desde el legislador europeo, se ha intentado establecer ese marco de referencia, que permitirá que **el titular de los datos tenga derecho a conocer el estado de los mismos**, con una obligación de mayor transparencia para las entidades que deciden usar ese conjunto de datos, considerando a tenor del artículo 9 los "datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud" como categorías especiales de datos personales.

La norma mencionada, en un intento de establecer un marco duradero en el tiempo, que como es habitual, y por el mayor avance de la tecnología, quedará en un tiempo desfasado, decreta la obligación para aquellas

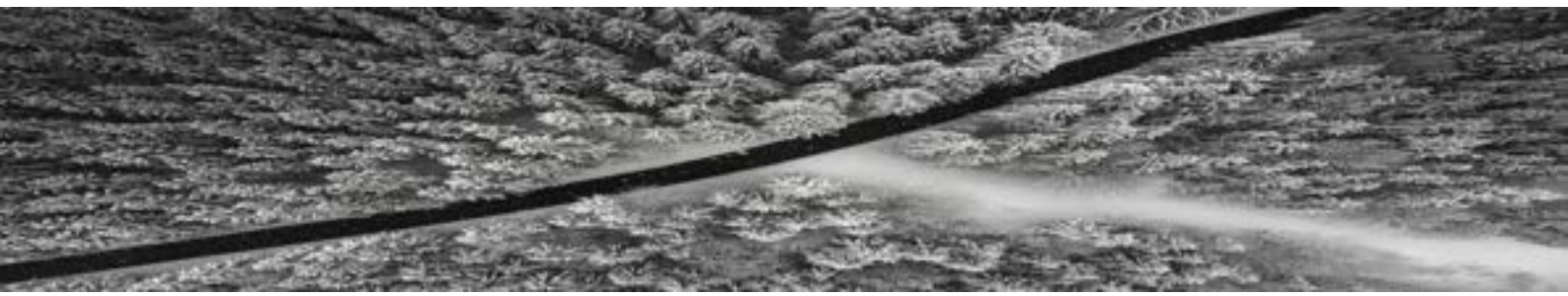
entidades que deseen tratar estos datos, de adoptar las medidas de seguridad tanto técnicas como organizativas, que sean acordes a los riesgos que el tratamiento de estos datos pueda suponer, sin decretar un catálogo cerrado, y es aquí donde el Blockchain, puede ser la solución. El Blockchain, al registrar bloques de información entrelazarlos mediante apuntadores hash puede contribuir a garantizar la integridad de la información, su trazabilidad, inviolabilidad, y fundamentalmente transparencia, al compartir la información de manera segura y posibilitar su recuperación en cualquier momento, por ser imborrable.

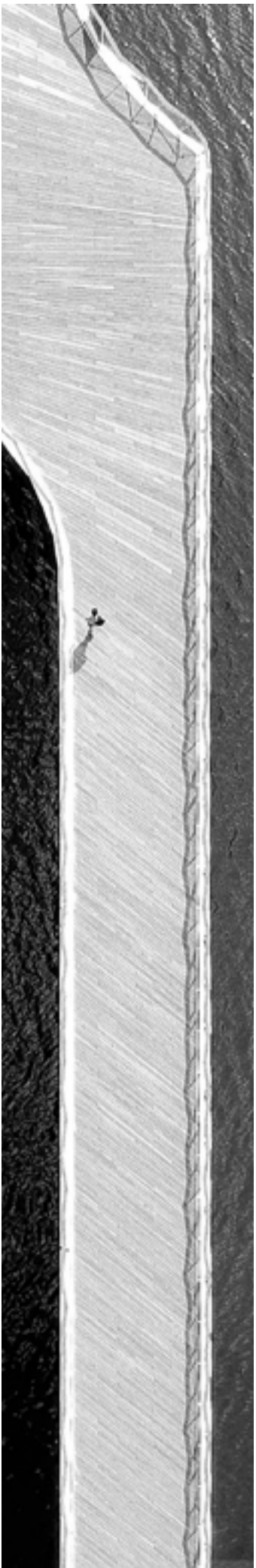
Además, **la utilización de Blockchain supone otras ventajas de gran importancia para los pacientes** como ahorro de tiempo, mantiene la integridad de la historia clínica enriquecida con información proveniente de múltiples fuentes de información, evita ataques informáticos que supongan accesos no autorizados a información especialmente sensible, facilita el poder determinar a qué información pueden acceder determinados profesionales sanitarios, y qué momentos, en resumen, un poder de disposición de la información en cualquier momento y lugar, enriquecimiento de la misma y seguridad en las transmisiones y conservación permanente.

Por otro lado, los agentes que intervienen en el mundo de la medicina se benefician de este sistema por la inmediatez en el acceso a la información del paciente, la actualización permanente de la misma y la mayor conexión y comunicación entre profesionales pudiendo contribuir a diagnósticos en menor tiempo, y mejorando la gestión de las organizaciones sanitarias como las listas de espera, ingresos, suministros de medicamentos, etc.

En la investigación y los ensayos clínicos, **la utilización de Blockchain supondría la disminución de los costes y del tiempo de desarrollo de futuros medicamentos**, mayor eficiencia y seguridad en la gestión de los registros y la protección de la información.

En resumen, el desarrollo de nuevas tecnologías aplicables al campo de la salud, es fundamental para el desarrollo de la medicina si bien es cierto que se deben arbitrar de manera pareja, las medidas que contribuyan a que el pacientes y las organizaciones se sientan cómodas y seguras en su uso a fin de mejorar y aumentar nuestra calidad de vida, siempre bajo el respeto a su integridad, intimidad, y derecho al honor, piedra angular de todo este sistema, que no es otro que el paciente.





DESCONOCIMIENTO DE LA LA FUNCIÓN PRINCIPAL DE LAS COOKIES

Javier Arnaiz y Silvia Ruiz, abogados de ECIJA

"Las Cookies son archivos que contienen pequeñas cantidades de información que se descargan en el dispositivo del usuario cuando visitan nuestra página web..."Este texto es habitual en la navegación de un usuario medio en las páginas web de los diarios, en las webs de compras e incluso en las entidades bancarias para hacer transacciones.

Las cookies son un tema de creciente interés (incluso con alguna campaña publicitaria de gran calado usándolas en tono cómico) pero realmente existe un gran desconocimiento sobre estos pequeños archivos.

Por intentar entender un poco más las funcionalidades de este tipo de cookies, **dentro del marco de la publicidad online,** podría mencionarse la monitorización de los hábitos en internet del usuario por el correspondiente prestador de servicios, información que va a ser utilizada para ofrecer todo tipo de productos y, simultáneamente, va a permitir realizar un perfilado con dicha información.

Como usuarios, en alguna ocasión aparece en pantalla un anuncio del increíble hotel en Canarias que se ha buscado previamente en una web especializada en viajes y, por sorprendente que parezca, ese hotel persigue al usuario casi diariamente recordando que efectivamente sigue ahí.

Este seguimiento, se realiza mediante la **instalación de esta categoría de cookies,** dicha observación se realiza en la mayoría de los casos de manera continuada, lo cual puede resultar muy intrusivo para los usuarios.

Este tipo de acciones publicitarias son bastantes habituales en el sector y podría ejemplificarse de la siguiente manera: Empresa A que quiere hacer una campaña publicitaria contrata a una Agencia B subcontratando a un proveedor C que incluye una cookie de análisis de comportamiento en una web D. Este entramado, es bastante habitual en el sector, pudiendo ser bastante más entrelazado en algunos casos.

La estratificación de este proceso, hace que el análisis del flujo de información de estas cookies, pueda resultar complejo y presente serias dificultades para poder demostrar el verdadero origen de la información.

Derivado de esta interacción, a partir de enero de 2019 comienzan a conocerse los primeros casos de Organizaciones sancionadas por incumplir el Reglamento General de Protección de Datos 2016/679, como consecuencia de la actividad de investigación y control de las correspondientes Autoridades Europeas de Control, garantes en todo caso de velar por el cumplimiento de la normativa en vigor.

En concreto, resaltar la reciente sanción impuesta por la CNIL (Comisión Nacional de Informática y Libertades) por un importe de **50 millones de euros** impuesta a Google, por incumplir la referida normativa, en concreto, por no haber informado correctamente a los usuarios sobre el tratamiento de sus datos personales, sobre la argumentacion de que la información que Google ofrece a sus usuarios, no es fácilmente accesible y se encuentra diseminada en diferentes documentos.

Tras el supuesto expuesto, añadir que cumplir con el RGPD en el marco de internet, está resultando ser un campo que se encuentra bajo la lupa de inspección y verificación de cumplimiento por las mencionadas Autoridades de Control, en parte por las propias reclamaciones de los usuarios que acuden a la Agencia competente, en defensa de su Derecho Fundamental a la Protección de Datos. En esta línea la última sanción

impuesta a una empresa española, en este caso por la Agencia Española de Protección de Datos (AEPD) durante el pasado mes de diciembre, sobre la base de que el correspondiente aviso de cookies implantado en su web no ofrecía la información relativa al uso de las cookies propias y de terceros, ni indicaba las finalidades para las que se utilizaba las cookies propias y de terceros.

Llegados a este punto, las fórmulas habituales de información en la primera capa al usuario en el banner de cookies (como la que se ha indicado al principio de este artículo) no ofrecen una información exacta al usuario por lo que **difícilmente va a poder conocer la finalidad del tratamiento de los datos** realizado a través de esas cookies instaladas en su dispositivo.

La problemática de la información sobre las cookies, es que los prestadores de servicios en numerosas ocasiones desconocen la verdadera funcionalidad de estos pequeños archivos por la complejidad del flujo de información mencionado anteriormente y difícilmente pueden informar al usuario final adecuadamente.

Otro punto a analizar es la o**btención del consentimiento del usuario para la instalación de estas cookies.** Con la entrada en vigor del RGPD y de la Ley Orgánica de Protección de Datos y Garantías Digitales se debería haber hecho más rígido la obtención de ese consentimiento al ser uno de los requisitos (no el único) para la legitimación de un tratamiento de datos (como puede ser la instalación de cookies). En el entorno web este consentimiento puede plantear dudas sobre si hace falta la configuración de una casilla para aceptar el uso de cookies o si serviría la mera navegación del usuario.

En línea de lo expuesto, la Agencia Española de Protección de Datos expuso en la décima sesión anual en junio de 2018 que:

“La fórmula habitual de “seguir navegando” podría seguir siendo válida si se refuerza la toma de decisiones sobre cookies”.

Bien es cierto que la fuerza normativa de esta sesión anual no es la misma de una guía, informe o resolución (puesto que las últimas guías a fecha de redacción del artículo siguen la normativa anterior y no han sido actualizadas al RGPD). No obstante, sí que puede hacer ver la intención del legislador de optar por una información en una primera capa, (eso sí, que pueda informar claramente la finalidad del tratamiento), para luego en una segunda capa optar por una información mucho más completa y que adicionalmente pueda configurarse por parte del usuario la instalación o no de las diferentes tipologías de cookies.

Esta doble vertiente está haciendo que el panorama de las cookies haya cambiado drásticamente en los últimos meses y se prevé que continúe cambiando conforme salgan nuevas guías o informes que ayuden a cumplir con la normativa. El **Reglamento de ePrivacy** puede reforzar este aspecto y debería reforzarlo, pues en muchos casos, la indefensión del usuario a la hora de estos tratamientos es muy amplia y no permite una toma de decisiones real sobre un aspecto tan fundamental como la privacidad.

THE ALGORITHMS ARE DARK AND FULL OF ERRORS

Dmitry Alekseev y Juan Diego Rincón, abogados de ECIJA

Besides the Game of Thrones reference in the title, this article is about a topic involved in everybody's daily life, but not understood enough. So, what exactly is an algorithm and why should I care?

In short, an algorithm is **a set of steps to perform a task or to solve a problem** – a tool of great relevance nowadays. In computer science, algorithms are series of steps that a computer program takes to perform a task [Data > Calculation > Answer/Result]. In this sense, the technology is an inseparable element of our daily life; for instance, a map application is capable of telling you how to get from point A to point B through a complex calculation, by using a route-finding algorithm involving location data of a user, a desired destination, and providing a result (e.g. all the options to get to your favourite coffee, from taking a cab to using public transportation). Essentially, that is the biggest benefit algorithms provide to the society: a shortcut from a problem to a solution by means of a computer code. The "thinking" capacity of a machine is what is known as "artificial intelligence" or "AI" - the ability of machines to work and react like humans (e.g. knowledge, reasoning, perception, planning and learning).

To perform a task, the machines must have **abundant information** in order to access objects, categories and relations between all of them, for the purposes of providing a result close to the common sense, reasoning and problem solving. The possibility of making inferences based on data by learning and adapting, understanding unstructured communications or documents provided by the user and autonomously and flexibly constructing a sequence of actions to reach a final goal without supervision is, broadly speaking, the "machine learning".

The power of such technology is **shaping the way we make decisions** and solve a vast amount of problems in short periods of time, but as AI changes major daily life issues, uncontrolled and unrecognized algorithms may have big consequences on a user's life. Examples include the determination by machines of who gets a job interview, who gets a loan and, in criminal cases, even who is likely to re-offend.

Doubtlessly, algorithms play an important part in our day-to-day life across all sectors and areas, being essential for technological advances. Targeted news and ads, face recognition, speech recognition, medical diagnosis and prediction are good examples. However, as algorithms are designed by humans and can learn from us, the **observation of individuals' behaviour and society as a whole** can lead to the inclusion of discrimination of any kind, whether related to race, gender or economic status, among others. The results, with meaningful impact in people's lives, can lead to extend, rather than mitigate, unjust biases. Then, are we leisurely becoming marionettes in hands of the logic behind automated decisions?

Aware of the opacity and the potential discrimination of the algorithms, the General Data Protection Regulation (GDPR) comes into play, trying to establish limitations on automated decision-making involved in the processing of personal data by mandating to inform concerned users whether such decision-making takes place, the logic behind, the significance and envisaged consequences. Although it would seem like there are precise obligations in this sense, none of those are focused on the actual method that leads to the answer or approach to a specific situation, presumably the cornerstone of the automated decision-making. Are the algorithms involved fair and transparent enough? And most importantly, to what extent do we need to know its functioning?

The GDPR illustrates with little-to-no explication on what exactly "meaningful information about the logic involved" is, forcing to search for clarifications in the European Commission's Paper on automated decision-making . According to such, the information about the logic involved must not be too technical, complex or confusing. The vast majority of the users do not hold a PhD in Computer Science; hence, there is no need to provide a source code of the algorithm or high-end description of the analytical processes in order to comply with transparency and information requirements under GDPR. Moreover, Stanford University student René F. Kizilcec conducted a research on the **relationship between the transparency of the algorithms and the users' trust according to the amount of the information given**, whose conclusion was logical: the right level of transparency is neither too little nor too much. Unfortunately, this undetermined indication is hardly applicable to everyday routine; for instance, how do we establish what information is provided and by what mean it is presented, considering the particularities of each data subject? And how such information can justify the decisions that affects individuals?

Sure enough, juggling with fair algorithmic and transparent, user-adapted information while making automated decisions and pursuing business needs is backbreaking. Public disclosure does not seem to be the best way of providing said information for blatant reasons: potential loss of competitive advantage, difficulty in benchmarking the bases for the explanation about the logic involved, or even a ploy to trick the system through the understanding of the decision-making. However, **what if there were an official and widely recognised certification system based on independent audits of algorithms?**

The idea is not new. Big firms have started to or already developed mechanisms for self-assessing algorithmic risks and fairness; O'Neil Risk Consulting & Algorithmic Auditing (ORCAA) is a former Harvard student's independent auditing company able to analyse how biased a certain algorithm is. Broadly speaking, the audit dives into the essential code of the algorithm, examining the quality and quantity of data processed (clean data, missing data, unreasonable data, etc.), the concept of success for the answer, the need for updates, the unintended consequences of the algorithms itself and many other factors. As a result, it provides a list of mitigation actions, improvements, enhancements and suggestions.

However, as per today, there is no global, independent organisation or institution for standardisation of algorithmic audits, similar to the ISO certifications, which would provide a **worldwide recognised certification for algorithms that are consistent** with a set of requirements and controls (similar to the ISO 27001). Even though this certification would not exempt a company using algorithms in processing of personal data from compliance with transparency and information requirements, it may establish a standard regarding the way in which such information is provided in cases of automated-decision making.

Audit and certifications may be a path for companies to guarantee the users that the use of their technology is responsible and founded and, at Even though this certification would not exempt a company using algorithms in processing of personal information from compliance with transparency and information requirements, the same time, improve the accuracy and development of such. There are many options, and technology can always do better. It is just a matter of having the right concerns and targets when implementing these tools in peoples' lives.

ETHICS AND THE PLACE OF HUMAN DIGNITY IN THE DATA PROCESSING OF THE FUTURE

Elena Peña, abogada de ECIJA.

From May 25th onwards, companies have been adapting their activity to achieve compliance with the new data protection legal environment, leaving them thinking the job is done. But now, in the spirit of the GDPR's principle of accountability, a new question arises: **should legal compliance be enough?**

The skyrocketing advances in the technologies that involve data mining in the past decade pose a threat to everyone's privacy and brings up to the long-standing debate regarding where the limits of these practices stand when they involve the processing of personal data.

This discussion gives way to the always controversial question: to what extent are we willing to permit the processing of our personal information, however intrusive, in exchange for being able to participate in social, administrative and commercial affairs? However, as companies are also a part of this equation, their responsibility must be taken into account. Therefore, the focus should be shifted from the individual "bargaining" with his or her data, to the rightness companies performing such processing.

The easy answer to that question would be the "plain legal compliance" one: as long as the processing of personal data carried out by the company is done pursuant to applicable data protection regulations, there is nothing that prevents it.

The decision in practice involves a much deeper assessment, and in the **decision-making process** the companies usually give weight to different economic, organizational and marketing aspects. The next step in the accountability path would be for companies, as players in our society, to go further from this strictly practical focus and consider if the processing is "good" or "bad".

This last concern and the resulting need to strike a balance between the **different interests at stake that involves a choice between a "good" or "bad" alternative**, or multiple "goods" and "bads," draws on the discipline of ethics. In this way, by shifting from a privacy-only approach, to one that includes the ethical perspective, the conversation moves beyond "are we compliant?" towards "are we doing the right thing?".

This growing **need for technology to go hand in hand with ethics** results in a big way from its impact in privacy. Such commitment originates from its connection to human dignity, which stands as the foundation for privacy and data protection. This translates into the need to treat the data subject not only as a consumer or user, but as an individual which deserves respect.

EDPS has acknowledged the significance of this matter by including the developing an ethical dimension to data protection in its Strategy 2015-2020, as it defends "accountability over mechanical compliance with the letter of the law", and that "feasible, useful or profitable does not equal sustainable".

An approach to reach this goal of ethical processing of data would be by using the legal obligations foreseen in applicable data protection laws as the grounds upon which to base the ethical analysis. In a European scope that would mean making use of the tools provided in the GDPR, in special, the test deriving from the **privacy by design principle and privacy impact assessments.**

To that account, in evaluating the potential impact of a new service or process that would involve the processing of personal data, the following questions, which have been distilled from various approaches to ethical decision-making, should be considered:

- Is it the option that best respects the rights of all stakeholders? This is the **Rights Approach.**
- Does this option treats people equally or proportionately? This is the **Justice Approach.**
- Will this option produce the most good and do the least harm? This is the **Utilitarian Approach.**
- Does this option serve best the community as a whole, not just some members? This is the **Common Good Approach.**
- Does this option lead me to act as the sort of company I want to be? This is the **Virtue Approach.**

Companies role in shaping the privacy reality should go beyond the mere respect of the law, and head towards the respect of the data subject as an individual. In this line, by way of ensuring a greater respect for human dignity and its safeguarding, the pervasive surveillance and the asymmetry of power which now confronts the individual could be counterweighted.

PRENDAS INTELIGENTES Y SU IMPACTO CON LA PROTECCIÓN DE DATOS

Esperanza López Prado, abogada de ECIJA.

Pasada la Navidad y en plena cuesta de enero, son muchos los ciudadanos que esperan con ansia las rebajas: una buena oportunidad para hacerse con ropa o accesorios inteligentes, cuyos precios originales suelen ser bastante elevados el resto del año. Y es que la tecnología ha revolucionado todo tipo de industrias y, entre ellas, la industria de la moda, incorporándose en la composición de prendas de ropa y complementos capaces de interactuar con los usuarios y obtener todo tipo de información sobre ellos.

Lo cierto es que las empresas de moda cada vez utilizan más la tecnología para innovar y distinguirse de sus competidores pero la cosa va más allá: **las prendas inteligentes, en su gran mayoría, recaban datos personales y analizan comportamientos y tendencias de los usuarios.** Se trata de información a gran escala, de big data y, en consecuencia, de poder. Poder para crear **perfiles, patrones y tendencias** que permitan conocer nuestros gustos y ofrecernos productos que, aparentemente, resultarán de nuestro interés. Pero no podemos olvidar que hay un elemento fundamental en juego: el derecho a la protección de datos personales.

En definitiva, las marcas tratan y explotan información de los usuarios que utilizan esta ropa conectada. Y es que los usos comerciales que se pueden llevar a cabo mediante la información recabada por este tipo de prendas son innumerables y, en ocasiones, ponen en entredicho la **privacidad y la seguridad** de dichos usuarios.

Cuando hablamos de prendas inteligentes hablamos de prendas aparentemente normales que llevan integradas funciones tecnológicas. Desde los ya "tradicionales" smartwatches o relojes inteligentes y pulseras de monitorización de ejercicio, hasta ropa que interactúa con nuestros dispositivos electrónicos con múltiples funcionalidades, trajes que permiten desbloquear teléfonos móviles o intercambiar tarjetas de contacto de forma digital, prendas que repelen líquidos y evitan manchas o que no mojemos en un día de lluvia, blusas y vestidos interactivos que se mueven cuando les hablamos o miramos, zapatillas que se adaptan a nuestro pie sin dejar huecos, etc.

Nos referimos también a chaquetas que, gracias a la **realidad virtual,** transforman el cuerpo en una interfaz y llevan a las personas a un planeta virtual de forma plena y que a su vez permite crear música por medio de los movimientos del cuerpo, o a bikinis que controlan el tipo de piel del usuario y la temperatura, enviándole advertencias de que deben echarse más crema solar o ponerse a la sombra. ¿La empresa que comercializa los bikinis tendrá capacidad para predecir las posibilidades de que sus clientes padezcan un melanoma? O, tal vez, **¿podría vender esa información a una entidad aseguradora** que, probablemente, pagaría una cantidad considerable por esa información?

También existen prendas de ropa que pueden servir de gran utilidad para **controlar la salud de los usuarios:** sujetadores deportivos, camisetas o calcetines que registran las distancias recorridas, las frecuencias respiratorias o el ritmo cardíaco, miden las calorías quemadas, el nivel de dióxido de carbono en el aire; camisetas de ciclistas que detectan síntomas de fatiga en la espalda y modifican su posición para evitar lesiones lumbares; prendas que permiten instalar un GPS y monitorear la forma de la pisada para prevenir lesiones; o prendas que monitorizan nuestras constantes vitales y pueden detectar riesgos de sufrir algún problema cardiovascular.

Igualmente, las prendas inteligentes han adquirido uno de sus papeles más relevantes en la moda para bebés: ropa que cambia de color cuando el niño tiene fiebre, patucos que miden sus constantes vitales o la frecuencia cardíaca, bodys que identifican irregularidades en el sueño, enfermedades respiratorias y defectos cardíacos e incluso pijamas que permiten detectar múltiples variables como la posición del niño, el nivel de actividad, su temperatura corporal o su ritmo respiratorio.

En relación con lo anterior, recientemente salía a la luz una polémica noticia que hacía saltar las alarmas. Y es que los uniformes de colegio ya no son lo que eran, al menos en China donde se están implementando **uniformes inteligentes equipados con chips que cuentan con una serie de sensores conectados a un sistema de geolocalización y de huella dactilar** y, a cámaras de reconocimiento facial, posibilitando a los profesores y a los padres localizar a los alumnos en todo momento, controlando su asistencia a clase. Además, el sistema de reconocimiento facial imposibilita que los alumnos se intercambien los uniformes para engañar a sus profesores. Asimismo, los uniformes detectan cuando los alumnos se quedan dormidos en clase y permiten hacer pagos en la escuela mediante reconocimiento facial o de huella dactilar para confirmar la compra, lo que posibilita a los padres controlar las adquisiciones de sus hijos e incluso establecer límites de compra a través de una aplicación móvil.
El debate en este caso surge no sólo del hecho de que se **monitorice a los menores dentro de la escuela,** sino también de la posibilidad de que la empresa que comercializa los uniformes pudiese utilizar la información recabada rastreando los movimientos del alumno incluso fuera del colegio.

Es indudable que la utilización de ropa conectada es cada vez mayor y que sus funcionalidades evolucionan a una velocidad inimaginable. Pero, realmente, **¿ponen las prendas inteligentes en peligro la privacidad de sus usuarios?**
Recordemos que l**a voz, la huella dactilar y la imagen son datos de carácter personal.** Y recordemos también que el tratamiento de datos personales exige el cumplimiento de la normativa que resulte de aplicación. ¿Qué ocurre, entonces, si las prendas inteligentes recaban la imagen, la huella dactilar y la voz de los usuarios? ¿Para qué se utilizarán y con quién se compartirán esos datos? ¿Se venderán a terceros? ¿Queremos que cualquier empresa en la que compramos un producto tenga nuestros datos y pueda explotarlos comercialmente?

Las entidades que van a explotar y comercializar los datos obtenidos a través de prendas inteligentes deben cumplir con las disposiciones de la normativa de protección de datos para evitar que se vea en tela de juicio la privacidad de sus usuarios. Para ello, deben contar con una **base que legitime el tratamiento** que se va a realizar, deben dar a conocer a los usuarios qué datos suyos se van a obtener y para qué se van a utilizar, quién los va a utilizar y explotar y, a quién se van a enviar, debiendo contar con el consentimiento previo e informado del usuario o con otra base de legitimación para el traspaso de datos.

Recordemos también que el tratamiento de datos personales de menores de 14 años requiere el **consentimiento de los padres** y que el tratamiento de categorías especiales de datos, como son los datos biométricos -reconocimiento facial y huella dactilar- o los datos de salud, requieren un consentimiento reforzado, es decir, el consentimiento explícito del usuario.
Igualmente, las organizaciones que utilizan estas tecnologías deben tener en cuenta la **privacidad desde el diseño y por defecto,** así como ofrecer ciertas garantías a sus usuarios, darles la posibilidad de oponerse al tratamiento de sus datos o de revocar sus consentimientos y aplicar en su caso, medidas de seudominización o anonimización que permitan que el usuario de las prendas inteligentes no sea identificable y se traten sus datos únicamente de manera agregada.

En definitiva, resulta evidente que el uso de la tecnología está en auge, pero la tecnología y la innovación deben ir de la mano de la privacidad, siendo necesario encontrar un equilibrio entre ambas. Es decir, las empresas de moda deben cumplir con la normativa para, entre otras cuestiones, no perder la confianza del cliente, evitando que su imagen y reputación se vean afectadas.

Son muchas las ventajas –en nuestra vida diaria, en la de nuestros hijos e incluso para nuestra salud- que puede traer consigo la utilización de prendas de ropa inteligentes pero, ¿estamos dispuestos los usuarios a renunciar a nuestra privacidad para poder disfrutar dichas ventajas? Y es que la responsabilidad no recae, únicamente, en los fabricantes de la ropa y accesorios conectados y en las empresas comercializadoras. **Los usuarios también somos responsables de conocer el uso que se va a hacer de nuestros datos** -y de los de los menores que los van a utilizar, en su caso-, debiendo leer las políticas de privacidad, las condiciones generales y los términos y condiciones de estas empresas y renunciando a su uso en caso de que no queramos que nuestros datos personales sean conocidos y utilizados por dichas empresas.

VIDEOVIGILANCIA: ¿CUÁNDO Y CÓMO?

Natalia Antúnez y Rubén Lahiguera Gallardo, abogados de ECIJA.

Hoy en día jardines de cámaras adornan nuestras ciudades. Se confunden con el mobiliario urbano y flanquean la entrada a numerosos establecimientos, museos, entidades bancarias, centros comerciales e incluso zonas de acceso restringido (como el recién estrenado Madrid Central).

La videovigilancia supone, en muchos casos, la monitorización de nuestro día a día y, lo que es más importante, la monitorización de los errores o descuidos que cometemos. El ojo omnipresente que todo lo ve.
Cabe preguntarse entonces si esta **intrusión tecnológica se encuentra justificada** y si existen límites o excepciones a su utilización.

En primer lugar, podemos entender la videovigilancia, desde la perspectiva de la protección de datos personales, como el tratamiento de la imagen y la voz de una persona a través de cámaras o videocámaras, fijas o móviles, bien, mediante su conservación en un sistema de información o bien mediante su retransmisión en tiempo real.
Sus fines pueden ser muy variados, abarcando desde la seguridad de bienes, personas e instalaciones, la captación de imágenes a efectos probatorios en un procedimiento judicial o administrativo hasta el control del tráfico o el control laboral por parte del empleador respecto a sus trabajadores.

Asimismo, para poder estar ante un tratamiento de datos personales lícito, este deberá cumplir con los principios regulados en el Reglamento General de Protección de datos (en adelante, RGPD). Por ello, la finalidad de la grabación ha de estar determinada por **motivo idóneo** (por ejemplo la seguridad), ha de ser necesaria (al no existir otra medida menos intrusiva e igual de eficaz) **y proporcional en relación a su alcance**, limitándose este al estrictamente necesario para cumplir el **fin perseguido** (no parece razonable, por ejemplo, la instalación de cámaras de videovigilancia para la seguridad de una instalación ubicando las mismas también en los vestuarios o baños de la misma).

Como consecuencia de esta variedad, las tipologías de estos tratamientos también son múltiples. Veamos algunos ejemplos:

Videovigilancia en comunidades de propietarios
Una de las peculiaridades de este tratamiento es la necesidad de que se alcance un acuerdo por parte de la Junta de Propietarios sobre la instalación de estos sistemas de seguridad, el cual servirá para delimitar el interés legítimo del Responsable (la comunidad de propietarios) en dicha instalación, respetando, eso sí, el principio de proporcionalidad respecto del **campo de captación de las cámaras o su plazo de conservación,** entre otras cuestiones.
Además, de acuerdo con el artículo 13 RGPD, es necesario informar al afectado del tratamiento que se va a realizar de sus datos, el cual se satisface con la instalación de distintivos o carteles en aquellos accesos en los que el tratamiento vaya a realizarse y sin que deba captarse la vía pública, salvo que sea indispensable por razón de la ubicación de las cámaras de videovigilancia.

Videovigilancia en el entorno laboral
Respecto a los requisitos para llevar a cabo este tratamiento, resulta interesante mencionar la Sentencia de la Sala 4ª del Tribunal Supremo de fecha 31 de enero de 2017 en la que, tomando la postura del Tribunal Constitucional, dicha Sala viene a confirmar los criterios para la válida implementación de sistemas de videovigilancia sin contravenir el derecho fundamental del empleado a la intimidad personal (art. 18.4 CE).
Concretamente, los requisitos son, en síntesis, haber satisfecho el derecho de información previa respecto al tratamiento y que se respete el **principio de proporcionalidad**, los cuales se entienden cumplidos incluso en aquellos casos en los que el empleado no ha sido expresamente informado sobre la finalidad referida a la monitorización de su actividad laboral, de acuerdo con las facultades que la Ley del Estatuto de los Trabajadores proporciona al empleador.

Cámaras “on board”
Un término que está adoptando cada vez más fuerza es la cámara “on board”, una cámara situada dentro

del vehículo o en el casco, permitiendo la grabación durante la conducción, o incluso con el vehículo estacionado. El resultado de dichas grabaciones puede ser bien para uso exclusivamente doméstico, uso ajeno a la normativa de Protección de Datos de Carácter Personal, o bien para su presentación como prueba en un procedimiento administrativo, o incluso penal, o para una grabación continuada y permanente en nuestro vehículo (videovigilancia "on board"), en las que sí aplicaría dicha normativa. Por esto último, la finalidad para la que va a ser destinada dicha cámara y el alcance de la misma resultan determinantes, ya que en caso de estar ante grabaciones en las que opera la normativa sobre protección de datos, debemos cumplir con lo establecido en el RGPD, y concretamente, con el principio de limitación de la finalidad y minimización de datos.

Drones

Resulta evidente que la utilización de aquellos drones equipados con cámaras, GPS u otros útiles capaces de captar y almacenar datos de carácter personal, puede vulnerar principios fundamentales, como el derecho a la intimidad, debiendo cumplir con los requisitos establecidos en el RGPD, y con medidas que garanticen la confidencialidad, integridad y disponibilidad de los datos recopilados. Asimismo, el Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil en su Anexo IX, establece los requisitos esenciales para aeronaves no tripuladas, que además de recoger que el diseño del dron ha de cumplir con los requisitos para su función, su uso no puede poner en riesgo la integridad de las personas, su privacidad, ni la protección de datos personales, en general.

Partiendo de esta base, debemos **distinguir entre sobrevolar un espacio público de uno privado**, ya que, en espacios privados, además de contar con los requisitos establecidos para poder pilotar la aeronave, siempre y cuando puedan ser grabadas terceras personas, la base legitimadora para el tratamiento de dichos datos será el interés legítimo del Responsable por seguridad de su propiedad privada y deberá informarse de la zona videovigilada.

Por otro lado, en espacios públicos, como regla general, el RGPD no permite la grabación con drones a civiles, ya que las características de dichas grabaciones se identifican con las establecidas para las videocámaras de la mencionada Ley Orgánica 4/1997 en la que las Fuerzas y Cuerpos de Seguridad del Estado tienen la competencia exclusiva para su colocación y utilización, por ello en caso que los drones sean titularidad de dichos Organismos Públicos operará el interés público, y en caso de ser de un civil, operará el interés legítimo del mismo, debiendo informar a los posibles terceros del perímetro videovigilado y contar con los requisitos establecidos en el RGPD. Por todo ello, dependiendo de la modalidad deberemos atender a distintas limitaciones, prohibiciones y condiciones de uso.

De todo lo anterior, cabe concluir que la tecnología y dispositivos que permiten la videovigilancia van evolucionando, y el RGPD no nos da respuestas concretas, ni sobre cómo poder realizar un uso adecuado y, por tanto, un tratamiento legítimo de datos, ni sobre qué medidas de seguridad corresponderían aplicar en caso de estar ante un tratamiento de datos legítimo. De ahí la necesidad de atender a las circunstancias del caso concreto en las que dicho recurso se vaya a utilizar y poder así adaptar las medidas idóneas para cumplir con la legalidad vigente.

Día Europeo de la Protección de Datos - Newsletter ECIJA

BIOMETRÍA, PROFILING Y PSD2.

Javier de Miguel y Beatriz Rodríguez, abogados de ECIJA

La **Directiva sobre servicios de pago (PSD2)** persigue, entre otros aspectos, la mejora de las medidas de seguridad implantadas por los proveedores de servicios de pago. Entre sus obligaciones, introduce la obligación de adoptar mecanismos de autenticación reforzada de los usuarios, mediante elementos tales como el reconocimiento facial, la huella dactilar o la huella de voz, cuyo impacto en materia de protección de datos implica mayores exigencias en dicho ámbito.

La Directiva PSD2 exige a los proveedores de servicios de pago, emisores de credenciales de seguridad personalizados, la adopción de medidas de autenticación reforzada de los usuarios, cuando concurran determinadas situaciones, tales como: el acceso a una cuenta de pago en línea, operaciones de pago electrónico o la realización de una determinada operación cuyas características puedan entrañar un riesgo de fraude. Así, la propia Directiva ha establecido tres elementos que permiten lograr la autenticación señalada: **conocimiento** (algo que el usuario conoce); **posesión** (algo que el usuario posee); e **inherencia** (algo que es inmanente al usuario), que deberán de ser usados (al menos dos de ellos de manera combinada) para llevar a cabo la referida autenticación reforzada exigida.

Si bien la normativa únicamente **exige la adopción de dos de los tres elementos propuestos** en caso de que optase por el relativo a inherencia, el proveedor de servicios de pago podrá optar por implantar mecanismos que supongan la obtención y tratamiento de datos que gozan de una especial protección por el Reglamento General de Protección de Datos (RGPD). En particular, el elemento de inherencia implica el tratamiento de datos biométricos, que permitirían al usuario acceder mediante su huella dactilar o el reconocimiento facial de su dispositivo.

Para el tratamiento de dichos datos, más allá de que deba tenerse en cuenta su especial criticidad a la hora de analizar los riesgos e impacto derivados de su tratamiento, la regla general es que el proveedor de servicio de pago deba obtener el consentimiento explícito del interesado, salvo que concurra cualquiera de las restantes causas legitimadoras previstas, cuya aplicación resulta compleja. **El consentimiento requerido solo será válido cuando el interesado haya sido informado al respecto; es decir, para poder prestar el mismo**, deberá conocer los aspectos relacionados con la obtención y usos de sus datos, de manera que, efectivamente, se consciente de que la utilización del elemento de inherencia conlleva la utilización de un dato biométrico, o consustancial a su persona.

Asimismo, no podrá entenderse que dicho consentimiento, exigido por la normativa de protección de datos ha sido prestado por la propia solicitud de los servicios de pago, toda vez que, el consentimiento explícito, exigido por la Directiva PSD2, no deberá entenderse como extensivo a la protección de datos, conforme establece la **European Banking Authority**. Por lo tanto, la causa legitimadora del tratamiento deberá de ser independiente a la propia solicitud de servicios de pago realizada por el usuario al proveedor de los mismos.

Es decir, que el consentimiento exigido por la normativa de protección de datos, ha de prestarse explícitamente para el **tratamiento de los datos biométricos para llevar a cabo la autenticación reforzada**, sin que pueda entenderse que la mera solicitud de estos servicios de pago, faculte al proveedor de los mismos para la obtención y el tratamiento de los datos biométricos del interesado.

Sin embargo, lo anterior no ha de implicar necesariamente la implantación de un mecanismo alternativo para la obtención referido consentimiento explícito, sino que

la mera elección del elemento de inherencia para autenticarse, siempre y cuando el mismo no sea exigido por el proveedor de servicios de pago, pudiendo, por tanto, el interesado optar por otros mecanismos de autenticación alternativos, podrá considerarse como una manifestación de la voluntad del interesado de someterse a este tratamiento de datos y por lo tanto, facultar al proveedor de servicios de pago para llevar a cabo el mismo, siempre y cuando, conforme se dijo anteriormente, el interesado haya sido previa y debidamente informado.

Asimismo, y sin perjuicio de lo anterior, la propia Directiva establece a su vez una serie de **exenciones a la obligación de la adoptar medidas para la autenticación reforzada del interesado**, entre las que se encuentra la posibilidad de no aplicar la misma cuando, tras la realización de un análisis de riesgos, se identifique que las operaciones de pago remotas arrojan un nivel de riesgo identificado como bajo, según los mecanismos de supervisión definidos.

En este sentido, para llevar a cabo el análisis de riesgos antedicho, los proveedores de servicios de pago podrán precisar la realización de un perfilado del usuario, teniendo en cuenta criterios como las pautas de gastos anteriores, historial de operaciones de pago, ubicación del ordenante y del beneficiario, así como identificación de pautas de pago anormales en relación con su historial. Es decir, el acceso a datos personales que serán tratados para la adopción de una decisión basada únicamente en un tratamiento automatizado, por medio de la elaboración del referido perfil. Circunstancia que conlleva, como en el caso anterior, la necesidad de contar con una **causa legitimadora** para poder desarrollar el tratamiento de los referidos datos personales del interesado.

Por lo tanto, en aquellos supuestos en los que exista una norma de derecho comunitario o de derecho interno habilite la realización del perfilado, la ejecución del mismo se considerará legitimada sin necesidad de que el interesado tenga oportunidad de oponerse. Sin embargo, y de manera similar a lo anteriormente indicado, sí será necesario **informar al usuario del perfilado llevado a cabo mediante la utilización de sus datos personales,** a fin de cumplir con el principio de transparencia establecido por la norma.

A la luz de lo anterior, la implementación de las medidas que PSD2 incorpora han de ser analizadas atendiendo a las disposiciones y limitaciones que la normativa de protección de datos establece. Siendo preciso, por tanto, que el proveedor de servicios de pago garantice que el tratamiento de datos está legitimado y que el usuario cuenta con información precisa y pormenorizada en relación con las finalidades perseguidas por los distintos intervinientes en las operaciones de pago, especialmente, cuando los tratamientos impliquen el tratamiento de sus datos biométricos o el análisis de sus hábitos de consumo.

Día Europeo de la Protección de Datos - Newsletter ECIJA

La evolución del deber de información respecto al tratamiento de datos de carácter personal

Joaquín Cives y Sonia Vázquez, abogados de ECIJA

Esta semana inundaba los medios la noticia referente a la sanción millonaria impuesta a **Google** por la CNIL por infracción de lo dispuesto en el RGPD. La autoridad francesa lo ha sancionado basándose, entre otros motivos, en la **información insatisfactoria proporcionada a sus usuarios con carácter previo a recabar y tratar sus datos**. El cumplimiento de esta obligación es uno de los pilares centrales en la normativa de protección de datos personales, ya que de ello depende la posibilidad por parte de los titulares de los datos de tener un control real de lo que se hace con su información. Las nuevas tecnologías, las diferentes plataformas digitales y la aparición de nuevos medios y canales a través de los cuales se puede obtener y tratar datos de carácter personal, han venido a complicar las posibilidades de los ciudadanos a la hora de saber qué se está haciendo realmente con su información personal, que es el derecho fundamental que trata de salvaguardar la normativa, lo que conlleva que las entidades que traten datos de carácter personal deberán articular correctamente el cumplimiento de su obligación de **actuar de forma transparente,** facilitando información accesible y compresible para los receptores de la misma.

Analizaremos a continuación la evolución de la regulación de esta obligación a lo largo de los años y su interpretación por diversas autoridades, en un intento de facilitar el cumplimiento de este deber de informar, no sólo en lo que a su contenido se refiere, sino también al modo de facilitar esta información a los interesados, de forma que se cumpla con el objetivo final de esta obligación, que no es otro que la **transparencia en el tratamiento de los datos personales.**

Inicialmente, la D**irectiva 95/46/CE transpuesta al ordenamiento español por la Ley Orgánica de Protección de Datos del año 1999**, establecían la necesidad de facilitar a los interesados la información referente al tratamiento de sus datos personales, indicando la existencia de un fichero, la identidad del responsable del tratamiento y de los potenciales terceros destinatarios, la finalidad del tratamiento y los derechos de los afectados, así como la referencia al carácter obligatorio o facultativo de las respuestas a las preguntas planteadas y la consecuencia de la negativa a suministrar los datos señalados. Además, sumaba dos puntos adicionales en aquellos casos en los que los datos no se obtuvieran directamente de terceros, **el contenido del tratamiento y la procedencia de los datos**. Por tanto, la idea básica era que el titular de los datos supiese de un modo muy sencillo quien trataba sus datos y para qué.

Esta normativa se mantuvo estable durante 20 años, pero, como se ha indicado, la imparable transformación digital de los modelos de negocio ha traído consigo posibilidades de gestión de la información a unos niveles que no podían ser previstos en el momento de aprobación de estas primeras regulaciones, por lo que este modo de facilitar la información difícilmente permitía a los ciudadanos conocer la realidad de los tratamientos en los que sus datos personales podían verse inmersos. Por este motivo, el legislador europeo decidió **ampliar la información que debe ser puesta a disposición de los interesados,** de modo que se permita una mayor constancia de los detalles relativos al tratamiento de su información personal y un mejor control sobre los mismos, ampliando además el catálogo de los derechos que les asisten frente a quienes hacen uso de sus datos.

Como consecuencia, el **Reglamento General de Protección de Datos** (Reglamento (UE) 2016/679) vino a introducir una serie de novedades muy relevantes en la cantidad y la calidad de la información a facilitar, reforzando este derecho de los titulares de los datos, al añadir una serie de puntos adicionales de información a facilitar en el momento de recabar datos de carácter personal, como son: **la base jurídica de tratamiento, el plazo o criterios de conservación de los datos, los datos de contacto del** Delegado de Protección de Datos, la existencia de transferencias

internacionales, el derecho a retirar el consentimiento otorgado, la posibilidad de presentar una reclamación ante la Autoridad de Control y la existencia de decisiones automatizadas o elaboración de perfiles con los datos personales. Cuando los datos no se obtengan directamente del interesado, se suma la obligación a incluir la referencia al origen y las categorías de datos tratados.

Sin embargo, en función del medio empleado para recoger información personal, desplegar toda esta información no siempre es sencillo, y además esta profusión de información puede llegar incluso a ser contraproducente.

Con el fin de clarificar y establecer un modelo a seguir, el Grupo de Trabajo sobre Protección de Datos del Artículo 29, autoridad europea en la materia, publicó las **"Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679",** posteriormente concretada por la Agencia Española de Protección de Datos, que publicó su propia "Guía para el cumplimiento del deber de informar", recomendando un modelo de información por capas, consistente en una capa básica y una segunda capa de información adicional, que vendría a desarrollar el contenido de todos los apartados preceptivos establecidos en la normativa. La capa básica contendría la información de forma resumida, permitiendo el acceso a la misma en el momento y en el mismo medio a través del cual se van a recabar los datos. Por su parte, en un segundo nivel, se presentaría de forma detallada el resto de informaciones, de un modo que permitiese su comprensión de forma sencilla. La finalidad de este sistema radica en facilitar a los responsables del tratamiento la configuración de los formularios y procedimientos (sin importar su formato), y por otro, en conseguir que las personas interesadas obtengan la información más relevante de forma rápida y simplificada, siempre en cumplimiento de los principios establecidos en el Reglamento.

Este fue el modelo seguido por la gran mayoría de entidades en sus procesos de adaptación a la normativa, que pasó a ser de plena aplicación el pasado 25 de mayo de 2018.

La reciente aprobación en España de **la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales** ha supuesto un respaldo definitivo a esta forma de dar cumplimiento a esta obligación ya que la misma regula de forma expresa esta posibilidad, pasando de ser una opción sugerida en las guías de las autoridades que interpretan la norma a convertirse en un precepto legal, con lo que se aumenta considerablemente la seguridad jurídica de quienes opten por este modo de dar cumplimiento a su deber de informar.

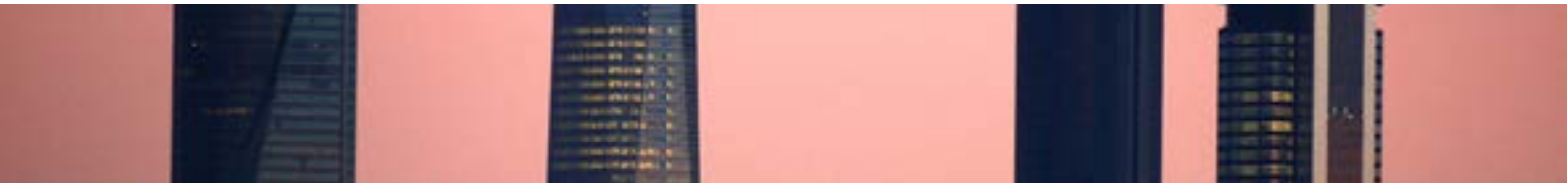
Pero, además, esta norma ha venido a introducir algunos matices respecto a lo indicado por la Agencia Española de Protección de Datos en su Guía, estableciendo en un contenido básico mínimo más reducido todavía, limitándolo a la **identidad del responsable del tratamiento**, la finalidad del tratamiento y la posibilidad de ejercitar los derechos.

Por tanto, el contenido de esta primera capa viene a quedar configurado de forma muy similar al inicialmente establecido por la Directiva y la Ley Orgánica 15/1999. De este modo, parece reconocerse tácitamente por el legislador la **imposibilidad existente en muchos casos de incluir toda la información pretendida por el Reglamento**, así como la ventaja que supone para el propio titular de los datos de conocer la información relativa al tratamiento de estos de forma sencilla, y que, sólo en el caso de que lo considere oportuno, pueda conocer en detalle las condiciones del tratamiento de su información personal.

No obstante, esta manera de informar ha de ser adoptada con mesura, ya que la minimización de la información facilitada debe realizarse únicamente cuando existan motivos que justifiquen la imposibilidad o dificultad de facilitar información adicional. En este sentido, cada situación debe ser analizada en **detalle, teniendo en cuenta diversidad de factores que obligarán en su caso, a** reforzar el deber de información, como podría ser el tipo de tratamiento a llevar a cabo o la tipología de datos tratados. Por tanto, ha de tomarse conciencia de que no existe una fórmula genérica a replicar en todos los tratamientos.

En esta línea, señalar que hay un principio establecido en el RGPD que viene a complementar esta idea y que todos los responsables del tratamiento deberán tener muy presente a la hora de cumplir con lo establecido en la norma, que no es otro que el **principio de responsabilidad proactiva.**

Este principio viene a subrayar la necesidad de los responsables de guiar todas sus actuaciones que impliquen el tratamiento de datos de carácter personal aplicando las medias necesarias para poder demostrar que el tratamiento cumple con la normativa, exigiendo un estudio previo y diligente del tratamiento a llevar a cabo. Sólo de esta forma, teniendo siempre presente la necesidad de actuar conforme a este principio, que implica **adaptar el modo en que se informa en función de los destinatarios**, se logrará realizar un tratamiento conforme a lo establecido en la normativa, garantizando a los titulares de los datos sus derechos, y alejándose de una potencial sanción por incumplimiento de las obligaciones establecidas.



Contacto

Área de
Privacidad y
Protección de
Datos de ECIJA

info@ecija.com
91.781.61.60

Pº Castellana 259C
Torre de Cristal
28046 Madrid
www.ecija.com

Esta newsletter ha sido elaborada por el área de Privacidad y Protección de Datos de ECIJA

www.ecija.com