ECIJA

8/ 02 / 2023

GUÍA DE TENDENCIAS EN MATERIA DE PRIVACIDAD

Área de Privacidad

www.ecija.com

España · Argentina · Brasil · Chile · Colombia · Costa Rica · Ecuador · El Salvador · Guatemala · Honduras · México · Nicaragua · Panamá · Portugal · Puerto Rico
República Dominicana · Uruguay

ECIJA es uno de los mayores y más reputados despachos españoles. En la actualidad se ha posicionado en el Top 10 de firmas nacionales por volumen de facturación, consolidándose como la firma española con **mayor presencia en América Latina**. Adicionalmente, ECIJA cuenta con una alianza estratégica con la firma internacional **Taylor Wessing**, que permite a ECIJA la cobertura global de las necesidades de sus clientes en 32 jurisdicciones.

ECIJA ha sido reconocida por los principales directorios internacionales (Chambers & Partners y Legal500) como **firma de referencia** en distintas áreas de práctica, destacada por la excelencia y la innovación en la prestación de servicios jurídicos.

Asimismo, **Financial Times** ha destacado a ECIJA como la **firma más innovadora de Europa continental.**

17
PAÍSES

"The Ibero – American giant"
Legal 500

35
OFICINAS

>1000
PROFESIONALES

ÁREAS DE PRÁCTICA

- Advisory
- Cumplimiento normativo
- Gobierno Corporativo
- Financiero
- Fiscal
- Laboral
- Legaltech
- Litigación y Arbitraje
- Mercado de Valores
- Mercantil / Fusiones y Adquisiciones
- Penal Económico
- Privacidad
- Propiedad Intelectual
- Público y Regulatorio
- Reestructuraciones e Insolvencia
- Tecnología, Medios y Telecomunicaciones
- Inmobiliario y urbanismo
- Sostenibilidad y Medio Ambiente
- Competencia y Derecho de la UE

SECTORES

- Distribución, alimentación y gran consumo
- Emprendimiento y Startups
- Energía y recursos naturales
- Entretenimiento y deporte
- Farmacia, salud y biotech
- Fundaciones y ONG´s
- Sociedades cotizadas
- TMT
- Ocio y turismo
- Private Equity y Venture capital
- Seguros
- Ciberseguridad
- Private Clients
- Derechos Humanos
- Gaming & Gambling

"ECIJA offers a very specialized service and always finds an answer to the problems we raise"

Chambers and Partners

RECONOCIMIENTOS

FT INNOVATIVE LAWYERS 2022

FT INNOVATIVE LAWYERS EUROPE 2022 WINNER

ECIJA, firma más innovadora de Europa Continental

THE LAWYER 2022

THE LAWYER

ECIJA, seleccionada en el top 3 de firmas en Iberia.

CHAMBERS EUROPE 2022

RANKED IN Chambers Europe 2022 Ecija Abogados

ECIJA, reconocida como firma de primer nivel líder en la edición de Chambers Europe 2022

CHAMBERS LATIN AMERICA 2022

RANKED IN Chambers Latin America 2022 ECIJA

ECIJA, reconocida como firma de primer nivel en la edición de Chambers Latin America 2022.

LEGAL 500 EMEA 2022

The Legal 500 EMEA TOP TIER 2022

ECIJA, reconocida como firma de primer nivel en la edición de Legal 500 EMEA 2022.

LEGAL 500 LATIN AMERICA 2022

The Legal 500 LATIN AMERICA TOP TIER 2022

ECIJA, reconocida como firma de primer nivel en la edición de Legal 500 Latin America 2022.

IFLR 2022

IFLR1000

ECIJA, reconocida como Firma de primer lider en la edición internacional de IFLR1000.

IBERIAN LAWYER 2022

Iberian Lawyer

TMT Law Firm of the Year in Iberia
Advertising Law Firm of the Year in Iberia
Digital Tech Law Firm of the Year in Iberia
E – Sports Law Firm of the Year in Iberia
Sports Law Firm of the Year in Iberia

EXPANSIÓN 2019, 2018, 2017, 2016

Expansión

ECIJA, ganadora de 7 premios Expansión a mejor Firma en Economía Digital, mejor Firma de IP y Protección de Datos y Firma más innovadora.

CINCO DÍAS 2022

CincoDías

Mejor Firma de Tecnología en España.

FORBES

Forbes

ECIJA, Firma del Año en Propiedad Intelectual y Nuevas Tecnologías (2017 – única edición).

EL REFERENTE

ElReferente

ECIJA, en el top 3 de mejores despachos de abogados en España para startups y venture capital según El Referente.

Índice

Coordinación: Daniel López Socio | Madrid, España

01. Punto de partida

En 2023 celebramos el **quinto aniversario de la plena aplicación del Reglamento General de Protección de Datos**, una norma que venía a regular en todos los Estados de la Unión Europea el respeto a los derechos de las personas sobre sus datos, posibilitando la consolidación y crecimiento de las empresas y el avance tecnológico.

En un momento en que en la mesa del legislador se encuentran futuras normas de gran calado, como el que será el **Reglamento sobre Inteligencia Artificial**, junto con otros como ***ePrivacy*** (que se ha vuelto un compañero, año tras año, como en el pasado ocurriera con el actual RGPD), adquiere una especial relevancia y acercamiento, desde la óptica jurídica y técnica a las tendencias que vienen en los próximos meses.

El uso de la **inteligencia artificial, los retos en materia de ciberseguridad, los flujos internacionales de datos, la adopción de la privacidad desde el diseño y por defecto, la cartera de identidad digital o el escenario *cookieless*, el uso de la biometría, los avances sobre el metaverso o la aplicación de la tecnología a campos tan importantes como la salud o el derecho**, plantean retos a los que, no sólo las asesorías jurídicas de empresas e instituciones, si no, los departamentos de sistemas y seguridad y el resto de áreas de las propias organizaciones, deberán dar solución, aprovechando las oportunidades que conllevan.

En el ámbito internacional, junto con los temas expuestos, en 2023 seguiremos avanzando con el desarrollo normativo. Los países que contaban con normativa específica en materia de protección de datos, en muchos casos, se encuentran actualizando su legislación avanzando hacia una nueva generación de normas. Finalmente, los que aprobaban sus normas en los últimos meses continúan madurándolas y aquellos otros que no contaban con un marco normativo específico, avanzan en el diseño y aprobación de sus propias normativas.

En Europa, las miradas están puestas en el nuevo marco que vendrá a regularizar las **transferencias internacionales de datos entre Estados Unidos y el viejo continente**. Ante años de incertidumbre, de adopción de mecanismos - invalidados posteriormente por el Tribunal de Justicia de la Unión Europea- parece que se vislumbra la luz al final del túnel, de contar con un mecanismo férreo que aporte seguridad jurídica a los interesados y empresas que se adhieran, junto con el necesario confort en el marco de la creciente economía digital (cabe recordar que dichas transferencias sustentan 7,1 billones de dólares, como indicaba, en su momento, la propia Casa Blanca).

Retos y oportunidades que, también, aparecen en la agenda de las autoridades de control en materia de protección de datos, con el debate de fondo de actualización de nuestro RGPD, queda avanzar en los mecanismos de colaboración y coherencia, en la búsqueda de soluciones a los problemas que se han puesto de manifiesto en los grandes procedimientos sancionadores (tanto a nivel europeo, como en Iberoamérica), o la colaboración con los delegados de protección de datos de las diferentes entidades, entre otros.

Un necesario enfoque multidisciplinar, la relevancia de los aspectos internacionales (no sólo de las propias empresas, si no, también de sus proveedores y terceros), la necesaria **innovación jurídica y el uso de la propia tecnología en el sector legal** (*legaltech*), jugaran un papel relevante.

A lo largo de las siguientes páginas, el equipo de TMT, Privacidad y Protección

de Datos de ECIJA España, irá analizando **los grandes retos y tendencias que se presentan en 2023**.

ECIJA como mayor Firma española en Iberoamérica, facilita sus servicios en estas materias con 25 años de4 experiencia en el ámbito de TMT y el conocimiento exhaustivo de los sectores de actividad de sus clientes.

Área de TMT, Privacidad y Protección de Datos
ECIJA Abogados

TENDENCIAS PRIVACIDAD

"The team provides seamless quality services independently of country specific laws and hurdles"

Chambers and Partners

02. Identificación basados en factores de Inherencia. Uso de sistemas de identificación biométrica desde la perspectiva de la protección de datos personales

Alonso Hurtado
Socio | Madrid - España

De un tiempo a esta parte el uso de sistemas de identificación basado en factores de inherencia no sólo se ha convertido en frecuente, sino que socialmente viene siendo aceptado por los ciudadanos el empleo de sistemas de identificación basados en su huella, su cara, o su voz, como sistema para tener acceso a multitud de sistemas electrónicos.

El incremento del fraude, especialmente tras la pandemia derivada del Covid-19, promovido principalmente por la realización de transacciones no presenciales, ha conllevado que tanto entidades del sector público, como del sector privado hayan apostado crecientemente por la utilización de sistemas de identificación y autenticación basadas en factores de inherencia, que en conjunto con otro tipo de sistemas hacen que el proceso sea más seguro.

Desde un punto de vista conceptual debemos tener presente la diferencia entre procesos de identificación y procesos de autenticación, siendo cada una de ellas dos partes de una misma moneda:

1. Identificación: proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica" (Art. 3.1 eIDAS)
2. Autenticación: proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o el origen y la integridad de datos en formato electrónico" (Art. 3.5 eIDAS)

El uso de sistemas biométricos para llevar a cabo los procesos iniciales de identificación de sujetos y posteriormente de autenticación de dichos sujetos (previamente identificados), con el tratamiento de datos personales que conlleva, es precisamente lo que plantea retos desde el punto de vista jurídico que los principales reguladores en la materia, tanto de Europa, como en otras jurisdicciones, han venido a poner de manifiesto.

Concretamente, el uso de sistemas de identificación biométrica plantea los siguientes retos desde el punto de vista del cumplimiento normativo:

1. La biometría como categoría especial de datos personales, en tanto el Reglamento General de Protección de Datos (RGPD).
2. La base legitimadora para poder tratar dicha tipología de tratamientos, en principio reservada exclusivamente al consentimiento en tanto tratamientos de categoría especial que son considerados conforme al (RGPD).
3. La información y transparencia previa al tratamiento de dicha tipología de datos, en tanto es determinante para poder validar que el tratamiento se realiza con todas las garantías para los ciudadanos.
4. La proporcionalidad de dicha medida, en función de la finalidad para la que vaya a ser utilizada, ya que es, probablemente, el juicio de valor más subjetivo y por tanto más interpretable que puede plantearse en relación con esta tipología de tratamientos de datos, siendo, posiblemente, el principal foco de conflictos.

Son diversos los pronunciamientos que se han venido produciendo durante los últimos años por parte de los reguladores en materia de protección de diversos estados miembros de la Unión Europea, así como por parte del *European Data Protection Board* (EDPB).

Entre los mismos se puede destacar una tendencia clara por parte del regulador, orientada a restringir el uso de este tipo de tecnologías al máximo posible, haciendo que el empleo de éstas siempre deba venir precedido de un análisis de proporcionalidad en relación con las finalidades perseguidas. Así como el sometimiento a una base legitimadora amparada en el cumplimiento de una obligación normativa que expresamente habilite el uso de este tipo de tecnologías para una finalidad concreta y específica (algo que no existe en la mayoría de las regulaciones del mundo por el momento), o bien ampararlo en el consentimiento expreso previo del titular de los datos.

Del mismo modo, por parte de los reguladores se pone de relieve la importancia de que la información proporcionada a los titulares de los datos, antes de proceder al tratamiento, sea realizada con un nivel de transparencia absoluta y extraordinariamente clara y comprensiva para todos los afectados, dando así cumplimiento al deber de transparencia que todo tratamiento, y particularmente de este tipo, deben cumplir.

Visto lo anterior, parece obvio que el nivel de conflictividad derivado del uso de tecnologías de identificación biométrica seguirá creciendo durante el año 2023, tanto a nivel europeo, como en otras jurisdicciones, abogándose por parte de ECIJA a que el uso de este tipo de sistemas sean debidamente regulados, dotando a un sector en claro crecimiento (dado el aumento de la demanda para reducir los riesgos derivados, especialmente del fraude, en multitud de sectores económicos) de la seguridad jurídica adecuada que permita afrontar las inversiones tecnológicas necesarias, todo ello en un marco de absoluto respeto y protección de los derechos y libertades de los titulares de datos personales.

03. Flujos internacionales de datos y su necesaria regularización

Daniel López
Socio | Madrid – España

El final de 2022 fue convulso en lo relativo a las transferencias internacionales de datos que las empresas realizaban, directamente o a través de sus proveedores. 2023 no iba a empezar de manera distinta, manteniendo en la agenda de empresas e instituciones la necesidad de regularizar los flujos internacionales de datos que realizan.

Si bien la aprobación de Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países, venía a adecuar el instrumento existente a la realidad y exigencias del Reglamento General de Protección de Datos, aportando una cierta seguridad jurídica para realizar estos tratamientos, como se ha evidenciado, no es un mecanismo infalible o seguro completamente.

Esto es debido a la diferente idiosincrasia derivada de los países a los que el exportador de datos (en sus diferentes roles de responsables, encargados o subencargados del tratamiento), atendiendo a qué cuenten con una normativa específica en materia de protección de datos o no. Del análisis de diferentes normas puede derivarse la imposibilidad de su efectividad, bien por ausencia de reglamentación posterior de autoridades de control, o mecanismos garantistas para la privacidad y protección de los datos de las personas.

A lo largo del año pasado, diferentes autoridades nacionales europeas, acordaron diferentes sanciones, de cuantías -en muchos casos- millonarias, en relación con la utilización de herramientas analíticas, educativas u otros servicios prestados por entidades estadounidenses, en las que el punto crucial eran las garantías para realizar transferencias internacionales. Aspectos que adquirían otra dimensión al establecerse en ocasiones la imposibilidad de utilizar las mismas, o la inmovilización de los tratamientos de datos realizados.

Uno de los casos que todos tenemos en mente (por las propias estructuras empresariales o derivado de la utilización de determinados proveedores) son las transferencias internacionales de datos, realizadas directa o indirectamente, a Estados Unidos. Una cuestión que parece contar con una solución en el horizonte cercano.

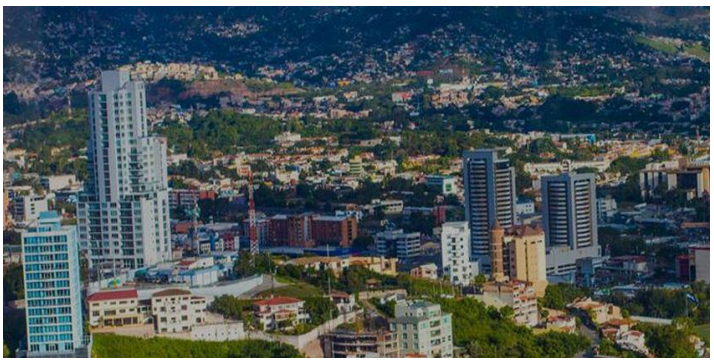
Con la vista puesta en los pronunciamientos europeos sobre Orden Ejecutiva que el presidente de los Estados Unidos firmaba el pasado 7 de octubre, que venía a aportar las necesarias garantías jurídicas para solucionar, por fin, un reto al que autoridades, empresas y organizaciones, se enfrentaban desde hace años para conciliar el respeto a los derechos de las personas y el avance tecnológico en una sociedad globalizada.

Pese a que Estados Unidos parece copar las titulares en este sentido, la necesidad de obtener garantías adicionales por parte de aquellos que desean exportar datos personales a terceros países afecta a otros países que directa o indirectamente, tratan datos personales por cuenta propia o de un tercero, viéndose afectados por las exigencias de la normativa europea.

De ahí, la necesidad de llevar a cabo las evaluaciones de impacto sobre dichas

transferencias, no sólo en lo relativo al análisis de la normativa vigente o pronunciamientos de Autoridades o Tribunales. Deben exigirse e implementarse medidas adicionales por exportadores e importadores de datos, tomándose como nivel de exigencia, lo recogido en nuestro RGPD.

Aspectos en los que, a nivel nacional, han venido trabajando diferentes países, con el ansiado objetivo de obtener el reconocimiento de un nivel adecuado de protección, como lo hicieran en los últimos tiempos Reino Unido (aunque no exento de polémica y cuestionamientos desde las autoridades europeas en relación con las modificaciones normativas que pudieran llevarse a cabo), Japón o la República de Corea. En este camino nos encontramos países como México, Colombia, Costa Rica o Marruecos.



No puede obviarse que, junto con los retos expuestos, 2022 también suponía el fin de las moratorias fijadas para la regularización de las transferencias internacionales mediante las Cláusulas Contractuales Tipo anteriores, por lo que en 2023 las empresas deberán hacer un examen profundo de aquellos tratamientos que implican estos movimientos internacionales, bien por su propia actividad, como la de sus proveedores.

En el ámbito iberoamericano, la propia Reb Iberoamericana de Protección de Datos, integrada por las autoridades nacionales con competencia en la materia, presentaba su modelo de cláusulas contractuales con el fin de estandarizar no sólo las garantías contractuales para los datos de las personas y sus derechos, si no aportar también la seguridad jurídica necesaria a las propias empresas e instituciones y los tratamientos que realizan en diferentes localizaciones. Un esfuerzo que vendrá a facilitar soluciones a los propios Estados, teniendo en cuenta las referencias normativas a la utilización de este modelo de regularización de transferencias internacionales de datos, tomando en muchos casos los estándares europeos (tal y como ocurre, por ejemplo, en Panamá).

Un mayor conocimiento, el análisis de los países a los que se pretende transferir para el establecimiento de garantías contractuales y, en su caso, llevar a cabo los procesos de redefinición sobre los flujos de datos, permite no sólo reducir los riesgos sancionatorios, si no adaptarse para los nuevos planteamientos de negocio y los retos de la economía digital.

Dentro de esos retos que se plantean a nivel internacional para las empresas, no puede obviarse la posible elaboración y aprobación de normas corporativas vinculantes, la elaboración de políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta, tal y como las define el propio RGPD.

Un mecanismo con, cada vez, mayor aceptación, atendiendo a las bondades y exigencias que conllevan, junto con el establecimiento de un sistema efectivo de cumplimiento en el seno de las entidades que, deben cumplir, con las exigencias normativas de los diferentes

Estados, incorporando todos y cada uno de los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

A la hora de afrontar la regularización de los flujos internacionales de datos, no pueden ignorarse otros mecanismos que, la propia normativa europea reconoce.

Los códigos de conducta, entendidos como herramientas que posibilitan acreditar el cumplimiento, la adopción de garantías (tal y como hemos ido analizando en el resto de los mecanismos), incluyéndose los aspectos concretos del sector de actividad de las entidades.

De igual manera, nuestro RGPD posibilita el establecimiento de mecanismos de certificación, que consideren, no sólo aspectos técnicos o relativos a la seguridad de la información (tal y como ocurre con determinadas certificaciones actualmente), sino también, aquellos aspectos jurídicos y organizativos que posibiliten garantizar el cumplimiento de las exigencias de la normativa europea y, por tanto, el respeto de los derechos de las propias personas, cuyos datos van a ser tratados.

Finalmente, el análisis de las diferentes temáticas que abordaremos en este documento debe entenderse como crucial para la identificación y regularización de las transferencias internacionales de datos. Aspectos como la información a facilitar, la legitimación para llevar a cabo los tratamientos pretendidos, la aplicación del principio de privacidad desde el diseño o la necesidad de conocer las diferentes normativas a nivel internacional y su desarrollo legislativo.

04. La insuficiencia de la ejecución del contrato como base de legitimación para la realización por la contraparte de cualquier tratamiento de datos relacionados

Esperanza López
Manager | Madrid - España

Javier de Miguel
Manager | Madrid - España

Las empresas que actualmente están basando el tratamiento de los datos de sus clientes o usuarios para el envío de publicidad personalizada, en la ejecución de un contrato en el que el interesado es parte, tendrán que pensárselo dos veces antes de continuar haciéndolo, a menos que estén dispuestas a exponerse a elevadas sanciones en materia de protección de datos.

Y, es que, la *Data Protection Commission* de Irlanda ha impuesto una sanción por importe de 390 millones de euros a Meta, al considerar que la forma en la que esta entidad pidió permiso en 2018 para usar los datos de las personas para anuncios personalizados en ambas redes sociales fue "ilegal" y, ha requerido a Meta a cumplir con la normativa de protección de datos, así como a modificar las bases legales sobre las que gestiona la publicidad en función de los datos personales de los usuarios "en un periodo máximo de tres meses".

En este contexto, el regulador irlandés ha aclarado que las entidades no pueden "forzar el consentimiento" de los usuarios para el procesamiento de sus datos ligándolo con la permanencia en la plataforma, de manera que, si no lo hacen, estarían obligados a abandonar la misma.

Por lo tanto, la citada sanción supone un punto de inflexión para las empresas, que establecen unos términos y condiciones muy amplios y generales, cuya aceptación resulta necesaria para la suscripción o contratación de sus productos o servicios, para tratar los datos de sus usuarios para múltiples fines (envío de publicidad, elaboración de perfiles, etc.), aun cuando los mismos no guardan ninguna relación con la finalidad principal que motiva el enrolamiento del cliente.

Toda vez que dichas empresas, únicamente, podrán tratar los datos que sean estrictamente necesarios para el desarrollo de la relación contractual, debiendo contar con una base de legitimación alternativa para todos aquellos tratamientos llevados a cabo para otros fines.

Por ejemplo, el envío de publicidad basada en una elaboración de perfiles previa, recurriendo a información obtenida de otras entidades o de la navegación del usuario, implica la obtención de dos consentimientos diferenciados:

(i) para envío de publicidad;

(ii) para elaboración de perfiles (a fin de poder remitir publicidad al usuario relativa a aquellos productos o servicios que realmente puedan interesarle), no pudiendo basarse en el mero enrolamiento del usuario, pese a que el mismo hubiese aceptado unos Términos y Condiciones generales en los que se informase de esta circunstancia, como parte del servicio.

Aunque este tipo de prácticas puedan resultar en ocasiones, beneficiosas para las empresas, especialmente las redes sociales, que monetizan basándose en la publicidad personalizada, en otras, a su vez, pueden dar lugar a cuantiosas sanciones por incumplimiento de la normativa de protección de datos.

Y, es que, desde la puesta en marcha del Reglamento General de Protección de Datos, la base legitimadora de ejecución del contrato para el envío de publicidad personalizada, entre otros fines, ha sido empleada de forma abusiva, lo que ha motivado la imposición de la sanción millonaria por parte de la autoridad irlandesa.

05. Nuevo paradigma de la ciberseguridad

Javier Arnaiz
Manager | Madrid - España

La ciberseguridad es un cuerpo normativo que ha estado íntimamente unido a la legislación de protección de datos. No obstante, en los últimos desarrollos europeos, ha tomado una importancia propia y cada vez más está siendo un campo en el que el regulador lo separa de los requisitos unidos al dato personal para adoptar una propia forma.

Si se menciona el caso concreto de España, de todos los países de la Unión Europea, puede ser uno de los que presenten una regulación más exhaustiva, incluyendo tanto normativa que proviene de Directivas y Reglamentos europeos, así como normativa propia y específica que es "exclusiva" del legislador español.

Y es que la normativa de ciberseguridad no solo afecta a aquellas entidades que traten datos de carácter personal (que ya quedan definidos como sujetos obligados por el Reglamento General de Protección de datos, 679/2016), sino que el abanico de entidades se ve ampliado a entidades del sector público, entidades privadas que presten servicios al sector público, proveedores de servicios digitales como mercados en línea, computación en la nube, buscadores en línea u operadores que gestionen servicios esenciales o críticos para la sociedad española.

En este marco de normativas "patrias" se puede encontrar el Esquema Nacional de Seguridad (ENS). El ENS ha recibo una nueva actualización en el pasado 2022 a través del Real Decreto 311/2022.

El objeto del ENS es determinar las medidas de seguridad en la utilización de medios electrónicos de las Administraciones Públicas, definiendo los principios básicos y requisitos mínimos que garantizan adecuadamente la seguridad de la información tratada y los servicios prestados. Como novedad, presenta la especificación clara de que dicha norma aplica a las entidades del sector privado cuando prestan servicios a sistemas de Administraciones Públicas sujetas al ENS.

Esta nueva versión del ENS viene a revisar (no de modo profundo) algunas medidas de seguridad actualizando, en algunos casos, los requisitos solicitados derivados de la propia evolución tecnológica.

A nivel europeo, también se puede ver una evolución en la normativa relativa a la ciberseguridad. El pasado 28 de noviembre de 2022 se aprobó oficialmente la nueva Directiva de ciberseguridad, sobre seguridad de las redes y sistemas de información (NIS 2 derivado de las siglas en inglés *Network and Information Security*).

NIS 2 viene a actualizar la actual Directiva sobre seguridad de las redes y sistemas de información, la conocida NIS. En este sentido, la nueva Directiva NIS 2 tiene por objeto definir las bases para las medidas de gestión de riesgos de ciberseguridad de carácter consolidado en los distintos Estados Miembros, es decir, la armonización entre los Estados miembros con respecto a la prevención, detección, y respuesta ante incidentes de seguridad (especialmente ciberataques dirigidos tanto a sector público como a sector privado cuando prestan servicios esenciales o importantes a la sociedad).

Cabe resaltar que entre las novedades de NIS 2 para reforzar dichos aspectos, destaca la regulación de medidas de supervisión más robustas, así como

nuevas obligaciones para los sujetos obligados como la realización de análisis de riesgos sobre la seguridad de los sistemas de información, la gestión de incidentes, continuidad negocio y gestión de crisis, la seguridad de la cadena de suministro o las obligaciones reforzadas de notificación y colaboración sobre incidentes y vulnerabilidades.

Con respecto a los sujetos obligados, además de los sectores que ya recogía la anterior Directiva NIS, NIS 2 amplía su ámbito de aplicación a nuevos sectores como los proveedores de redes o servicios públicos de comunicaciones electrónicas; los de gestión de aguas y residuos; aquellos relativos a la fabricación de productos electrónicos, ópticos y los fabricantes de vehículos; sector de la alimentación o los servicios digitales, ampliando a plataformas de servicios de redes sociales y centros de proceso de datos.
NIS 2 forma parte de un paquete de normas europeas enfocadas en materia de ciberseguridad, entre las que destacan el reciente Reglamento aprobado sobre la resiliencia operativa digital para el sector financiero (el Reglamento DORA) y la Directiva sobre la resiliencia de las entidades críticas (CER).

En resumen, puede verse como la regulación que afecta a la ciberseguridad cada vez se va ampliando y definiendo su propio ámbito de aplicación; dicho esto, como ha podido comprobarse en este artículo, su ámbito de aplicación cada vez está más dirigido a entidades concretas que presentan un riesgo para la sociedad actual alejándose de fórmulas genéricas (que se han visto en el pasado como no conseguían el objetivo perseguido por el legislador).

Como conclusión, aquellas entidades pertenecientes a un sector de actividad tecnológico o con riesgo para la sociedad han de tener en cuenta estos nuevos requisitos, ya que, cada vez más, los estándares y normativas para proteger las infraestructuras, servicios e información, se van a ir haciendo más comunes y exigentes.

06. Retos y tendencias en seguridad de la información

Jesús Yáñez
Socio | Madrid - España

La seguridad en el tratamiento de los datos de carácter personal no es un nuevo reto específico para este 2023, pero sí una materia que necesita mejorar notablemente en nuestro país si atendemos a las cifras que arrojan distintos informes[1] sobre incidentes de seguridad durante el 2022:

- El 38% de las empresas españolas ha sufrido al menos 10 incidentes o brechas de ciberseguridad.
- La escasez de competencias en ciberseguridad afecta actualmente a más del 9 de cada 10 empresas españolas (96%). El mayor reto al que se enfrentan en materia de ciberseguridad es la falta de ciber profesionales cualificados.

Estamos por tanto ante un caldo de cultivo preocupante, ya que, a la falta de personal cualificado se une el hecho de que los incidentes y brechas de seguridad siguen aumentando exponencialmente, teniendo en cuenta que las cifras indicadas solo reflejan brechas e incidentes detectados, no aquellos ni siquiera detectados, situación muy habitual en el tejido empresarial español, compuesto en gran medida por pymes y micropymes, cuya inversión y gestión en materia de ciberseguridad es escasa.

Debe tenerse en cuenta que la normativa de protección de datos establece la necesidad de implementar medidas de seguridad técnicas y organizativas en el tratamiento de datos de carácter personal, y que dicha obligación es una obligación de medios, y no de resultado tal y como ha confirmado el Tribunal Supremo. Esto se traduce en que, mientras el responsable o el encargado del tratamiento puedan demostrar que aplicaron medidas de seguridad teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, incluso en el caso de un suceso que afecte a la confidencialidad, integridad o disponibilidad de los datos personales, no habría infracción del artículo 32 del RGPD.

No deja de ser una consecuencia más del principio de responsabilidad proactiva: gestionar riesgos y tratarlos en consecuencia, incluyendo aspectos de seguridad tanto organizativa como técnica.

El propio RGPD es parco en establecer medidas de seguridad concretas, pero se fija en los estándares internacionales

[1] Cifras extraídas del informe "What's Next in Cyber", de Palo Alto Networks.

en materia de seguridad de la información para la aplicación efectiva de medidas. Además, debemos fijarnos en la tendencia del legislador: Desde 2016 se ha producido un importante desarrollo normativo en materia de ciberseguridad en Europa y en España cuyos sujetos obligados son especialmente administraciones públicas y sus proveedores (ENS), sectores financieros, asegurador, y otros servicios esenciales a través de Directivas y Reglamentos (como las recientes NIS 2 y DORA), y guías sectoriales de la Autoridad competente de dichos sectores. No obstante, se espera que en los próximos años cada vez sean más los sectores que sean sujetos obligados de estas normas, tratando de homogeneizar un nivel adecuado de seguridad de la información en Europa generalizado.

Para acreditar nuestra responsabilidad proactiva en materia de seguridad, nada mejor que la implementación de sistemas de gestión de seguridad de la información basados en estándares internacionales, y a ser posible certificados (ISO 27001, ENS, Sellos de privacidad europeos, o *framework* en materia ciberseguridad de ENISA), incluyendo la gestión y compromiso de nuestros proveedores en materia de seguridad de la información debido a la dependencia tecnológica cada vez más creciente que tenemos.

No vamos a obtener la certeza de no sufrir una brecha de seguridad, eso es imposible, pero sí vamos a poder acreditar una gestión adecuada, daremos una mayor confianza a nuestros clientes y proveedores, y evitaremos sanciones en la materia.

07. Procesos de identificación y su incidencia en materia de protección de datos

Joaquín Cives
Manager | Madrid - España

La diligencia en la identificación de los clientes para evitar suplantaciones de identidad en los procesos de contratación seguirá siendo uno de los principales focos de atención por parte de la Agencia Española de Protección de Datos.

Este tipo de fraudes sigue creciendo de manera exponencial y afecta especialmente a las grandes empresas que realizan, de forma masiva, procesos de contratación a distancia. Algunas de las modalidades de este tipo de delitos, como el SIM Swapping, que afecta a los sectores de banca y telecomunicaciones, provocan graves perjuicios económicos a los afectados.

La AEPD interpreta estas contrataciones fraudulentas como un incumplimiento de la normativa de protección de datos personales, tanto desde un puesto de vista de la seguridad como desde la perspectiva de la legitimación de su tratamiento y, si considera que no ha habido una diligencia suficiente en el diseño o la ejecución del proceso de identificación, viene sancionando a las entidades afectadas.

Durante el año 2022 todas las grandes operadoras de telecomunicaciones fueron objeto de fuertes sanciones por esta causa, y es de esperar que esta tendencia se mantenga en el nuevo ejercicio, dado que la Agencia tiene como objetivo tratar de evitar que se sigan produciendo supuestos de suplantación de identidad.

La problemática es compleja, por cuanto el uso de sistemas de identificación robustos (como el uso de la biometría o la realización de copias de los documentos acreditativos de la identidad) han sido también objeto de sanciones por la Autoridad de Control, que los considera contrarios al principio de minimización en el tratamiento de los datos, por lo que habrá que estar atento a nuevas resoluciones o la aparición de nuevas normativas que aporten seguridad jurídica en un tema de especial relevancia para todos los implicados.

08. Tratamiento datos y su protección en el ámbito de los wearables

Lorea Roncal
Asociada Senior | Pamplona - España

Si bien los primeros hitos de la tecnología *wearable* se enmarcan en los *"early sixties"* (audífonos, calculadoras, relojes, …) no sería hasta bien entrados los 2000 que el desarrollo de esta tecnología en distintos soportes permitió no solo la ampliación de los usos de aquellos, sino también su generalización, y, por tanto, la capacidad de llegar a un abanico de usuarios tan amplio como variado. Haciendo de la tecnología *wearable* una herramienta a disposición del consumidor medio, y, por tanto, dejando de ser un ideal y un instrumento limitado a ciertos estratos de la sociedad.

Pero, partamos de la definición de lo que son los soportes o tecnología *wearable*, para poder desarrollar a posteriori los tipos de dispositivos existentes, así como los beneficios y los peligros del uso de este tipo de tecnología en su vinculación con el tratamiento y la protección de datos.

La tecnología *wearable* (anglicismo que viene a designar la tecnología "ponible" o "vestible") se trata del uso de dispositivos electrónicos inteligentes incorporados al cuerpo de distintas maneras, sean en "soporte" textil (ropa inteligente / tecnológica), soporte electrónico (gafas, pulseras, smartwatch, cámaras), u otro formato, usado corporalmente (implantes o accesorios) siempre y cuando interactúen como extensión del cuerpo o mente del usuario, permitiendo la recogida, tratamiento y uso de datos del usuario referentes a hábitos, salud, costumbres, rutinas de quien lo lleve, y en ocasiones, de terceros que desconocen tal recogida, tratamiento y uso de datos personales.

La Agencia Española de Protección de Datos aborda en las distintas guías publicadas[2] la tecnología wearable, indicando que el uso de este tipo de tecnología ha de venir legitimado por normativa habilitante al efecto, estando prohibida en caso contrario, dado que no queda enmarcada en el ámbito estricto de la salud pública, ni de la vigilancia de la salud derivada de la prevención de riesgos laborales, siendo así que el tratamiento que deriva de la recogida de datos por medio de tales dispositivos, supone, entre otros, el tratamiento de datos de salud, entendiendo como tal una categoría especial de datos, la cual sin una base jurídica como es el cumplimiento de una norma legal, no cuenta con una legitimación amparada en la normativa vigente de protección de datos, vulnerando los principios que rigen la mentada (Articulo 5 RGPD3) en cuanto al uso, tratamiento y almacenamiento de datos de carácter personal; licitud, consentimiento, calidad, información, proporcionalidad y responsabilidad.

La fusión del ser humano con los microprocesadores hace posible la aplicación de la tecnología *wearable* en distintos escenarios, siendo los más

[2] Guía de Orientaciones procedimientos anonimización de datos//Guía de Seguridad y Privacidad en Internet //Guía sobre protección de datos y relaciones laborales

[3] 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 (Reglamento general de protección de datos)

comunes planteados por las autoridades de control los siguientes:

- La tecnología para llevar puesta (*wearable computing*);
- Los dispositivos móviles que registran información relacionada con la actividad física de las personas;
- Dispositivos de videovigilancia y domótica (oficinas y hogares con detectores, termostatos y sensores conectados, y cámaras integradas en vestimenta profesional que permiten el control y optimización del desempeño de las labores profesionales con el estado de salud del propio trabajador).

Cabe resaltar que el uso de microprocesadores en la tecnología *wearable* ha de estar dotado de la característica primordial de ser "vestible", es decir, un e-book dispone de microprocesadores, una *Smart TV* también, pero ninguno de ellos es vestible o llevable, como lo es un smartwatch, pulsera o gafas, razón por la que estos ultimo si se consideran productos wearables.

El uso de cámaras y termostatos, así como de dispositivos GPS, en el ámbito laboral, como dispositivos integrados en uniformes profesionales exigida en algunos puestos de trabajo, como son los cascos de bomberos, las cámaras integradas en determinados gruistas, o los termostatos vinculados a uniformes laborales, permiten la mejora en la seguridad laboral y una mayor optimización de medios y recurso, sin olvidar un mayor control de la vigilancia de la salud del propio trabajador.

La legitimación de tratamiento de los datos recabados de esta manera se fundamentaría en el cumplimiento de una exigencia legal imperante y determinada por normativa vigente (Laboral, PRL y/o vigilancia de la salud) dado que dejarlo al consentimiento del trabajador, podría llegar a entenderse que no hay una igualdad de posiciones, pudiendo concluir que tal consentimiento no ha sido otorgado de manera libre, voluntaria e inequívoca.

Por tanto, los peligros del uso de esta tecnología en el ámbito laboral y las consecuentes medidas de seguridad adicionales a implantar deberán ir encaminadas a la limitación de finalidad, el borrado de datos toda vez la finalidad haya sido ejecutada, así como la minimización y proporcionalidad del tratamiento de datos. Se podría aplicar por analogía el procedimiento, medidas y acuerdos que hoy en día se aplican al BYOD, poniendo en práctica tales directrices para un sistema WYOD (*"Wear your own device")* en el ámbito laboral.

En cuanto a los escenarios antes planteados de *wearable computing* y uso de dispositivos móviles que registran información relacionada con la actividad física de las personas, hemos de centrar nuestro estudio en la recogida, guarda y tratamiento de los datos recabados por este tipo de dispositivos:

Tipos de dispositivos *wearables*

- Gafas Inteligentes: controladas a través de voz, que permiten hacer fotografías y grabar videos de todo aquello que estemos viendo y reproducirlos en otro instante, consultar correo electrónico, el tráfico, noticias o la ruta más corta para llegar a un punto del mapa, traducir a cualquier idioma los carteles cuya imagen sea capturada y realizar una videoconferencia en directo.
- Accesorios y complementos: relojes y pulseras activados por huella o voz, que permiten recabar y guardar toda la información relativa al modo de vida, hábitos de consumo (permiten realizar pagos por medio de dispositivo), costumbres (hábitos deportivos, rutas realizadas, ritmo cardíaco, ciclos de sueño…)

- Industria textil: prendas que indican la temperatura de quien las lleva, que contabilizan los kilómetros recorridos, la ruta, ritmo cardiaco, prendas de se iluminan para ser vistos en zonas oscuras, que mejoran movimientos corporales o corrigen respiraciones y movimientos musculares en el ejercicio de determinado deporte.
- En el ámbito de la medicina y la salud: dispositivos de tecnología *wearable* que implantados en el usuario controlan y registran niveles de glucosa, dispensadores automáticos de insulina, control de tiroides, reguladores de hormonas; información recabada por dispositivos llevables, y transferida a ordenadores y dispositivos a los que puede acceder todo un equipo médico, independientemente del país donde ambos actores (Pacientes y médicos) se encuentren.

Datos recabados y limitación de uso

La tecnología *wearable* expuesta como antecede permite recabar todo tipo de datos tal y como hemos referido, sin embargo, son los datos de salud los que mayores implicaciones legales pueden llevar. El análisis de riesgos pertinente a llevar a cabo cuando usamos este tipo de tecnología nos lleva a analizar el tipo de datos recogidos, la finalidad para que la que se recaban (no es lo mismo recabar con una finalidad de optimización del estado de salud, que con la finalidad limitada a un momento concreto como puede ser un entrenamiento para una carrera, o el uso de tales datos para mejorar el precio y/o prestaciones de un seguro o cobertura sanitaria. De ahí que la finalidad la ha de determinar el usuario, siendo el dispositivo y sus funcionalidades los que queden limitados a lo que el usuario determine y no viceversa.

Acceso, conservación y transferencias de datos

Al mismo tiempo será el usuario quien determine quién accede a tal información (Limitación de accesos) y con qué rol, pudiendo modificar estos roles y accesos a su voluntad, impidiendo el acceso y uso por terceros no autorizados.

Los datos serán guardados en tanto en cuanto puedan derivarse diferentes responsabilidades del tratamiento, si bien, el usuario ha de conocer no solo la información recabada, sino también durante cuánto tiempo se conservará y dónde; dado que determinados dispositivos se encuentran alojados en servidores ajenos a la UE, lo mínimo que el usuario ha de conocer es dónde y hasta cuándo van a ser guardados estos datos, sin olvidar que su uso queda limitado a la finalidad inicial de recogida, no pudiendo utilizarse para finalidades adicionales o ajenas a las prestablecidas (como *profiling* o perfilados de consumo) con el conocimiento y consentimiento previo y expreso del usuario.

Concluimos con la siguiente reflexión: La tecnología *wearable* ha venido para quedarse, está claro, si bien los usuarios no son conscientes de la magnitud y la trascendencia que tiene la recogida de sus datos (salud, hábitos y consumo, entre otros) y su tratamiento por parte de terceros como son prestadores de servicios en internet, compañías aseguradoras e incluso sector bancario.

La normativa de protección de datos es clara al respecto; cumplimiento de los principios que rigen la norma y tratamiento de datos en cualquier esfera (Articulo 5 RGPD), procedimentado de la recogida, estableciendo pautas de legitimación (cumplimiento legal, consentimiento o cumplimiento contractual), plazos de guarda y ubicación de los datos una vez sean recabados y guardados, así como las pautas a seguir en la eliminación total y efectiva de aquellos.

La minimización, limitación y la proporcionalidad con los criterios imperantes en la ponderación de lo que para el usuario puede ser meramente baladí y el interés real de los prestadores de servicios en disponer y utilizar la información recabada, para fines que van mucho más allá de la voluntad y conocimiento del usuario.

El espectro de uso de la tecnología *wearable* en los múltiples dispositivos existentes en la actualidad y su disponibilidad por el consumidor medio han hecho que el "*no limit for default*" sea un principio imperante cuando debería ser la excepción de la norma.

Es indudable que las nuevas tecnologías optimizan y mejoran nuestro día a día, pero seamos conscientes de lo que hacemos, lo que cedemos y del precio que pagamos por ello.

09. Innovación y *Privacy by Design*

María González
Socia | Madrid - España

Estamos en un momento en que la tecnología y el desarrollo de diversas funcionalidades forman parte del día a día de los usuarios, los ciudadanos, las empresas y las administraciones públicas.

La tecnología se encuentra en un momento en que es cada vez mayor la capacidad de almacenamiento, pero, sobre todo, de explotación de los datos que son recabados en el día a día de la sociedad a través de todo tipo de dispositivos electrónicos y tecnológicos (teléfonos, ordenadores, relojes y pulseras inteligentes, televisores, o electrodomésticos entre otros). La capacidad de almacenamiento, de explotación, la consumerización de la tecnológica, lleva aparejada la capacidad de generar y desarrollar diversas funcionalidades, que, en muchos casos, conllevan un alto impacto en la privacidad de los usuarios.

Si bien dicho impacto no debería ser un obstáculo para el desarrollo y puesta en producción de dichas funcionalidades como soporte y mejora el día a día de la sociedad, son cada día más las normativas que ponen foco en la protección de la privacidad, más allá del RGPD, la LOPDGDD, o normas específicas como la de tratamiento de datos personales por las fuerzas y cuerpos de seguridad del estado. Encontramos, además, normas sectoriales (como regulación financiera / seguros, regulación sanitaria, etc.), y aquella enfocada a la regulación propia de la tecnología y la innovación tecnológica (DSA, DMA, IA, …) que ponen especial atención en los aspectos más críticos relacionados con la protección de la privacidad e intimidad de los usuarios en la utilización de tecnología.

Así en 2023, la privacidad seguirá siendo un aspecto esencial dentro de la protección de los derechos e intereses de los usuarios en el uso de la tecnología, tanto de forma personal y directa, como de forma indirecta pues el uso de la tecnología es realizado por entidades privadas y administraciones públicas, para conocer mejor al usuario, dotarle de servicios más personalizados, etc.

Aunque no es novedad, cobran especial importancia y relevancia, la implantación y realización de procesos de "*Privacy by Design*", que permitan que las funcionalidades y aplicaciones que conllevan el desarrollo de la tecnología y la explotación de los datos, no solo protejan la privacidad e intimidad de los usuarios (derecho fundamental), sino que aporten nuevas soluciones que permitan la mejora de ámbitos tan importantes como por ejemplo, el de la salud, con herramientas que permitan un mejor seguimiento, la mejora de diagnósticos, de la investigación médica, y por supuesto, la mejora de los tratamientos llevados a cabo.

Estos *Privacy By Design*, deberán también normalizarse en el desarrollo de sectores como el *retail*, financiero-asegurador, y cualquier otro en donde el consumidor es el eje principal, pues en estos casos el conocimiento del usuario, derivado de su seguimiento, el conocimiento de sus gustos, intereses, aficiones… permitirá el desarrollo de productos y servicios más ajustados e interesantes para el consumidor, y también aumenta la capacidad de promocionar, comunicar y dirigir los productos desarrollados al público objetivo concreto.

Pero, los *Privacy By Design* no son solo importantes y esenciales en aquellos sectores o desarrollos dirigidos a usuario y/o consumidor final, también en aquellos sectores y actividades donde, si bien a priori no se tratarían datos personales, pueden existir aspectos concretos que por seguridad jurídica de las entidades requieran de estos análisis exhaustivos.

No debemos olvidar en este 2023 que la falta de cumplimiento de la normativa de protección de datos y materias relacionadas no sólo supone riesgos de carácter económico, sino que existe un riesgo aún mayor relacionado con la falta de confianza de los usuarios, los daños en la imagen y reputación corporativa, etc., que hacen que la implantación de procesos de *Privacy By Design* sean claves en el desarrollo empresarial y social.

10. Cartera de identidad digital europea

Mar Ibañez
Manager | Madrid - España

Para incrementar el uso y la eficacia de los servicios electrónicos en la Unión Europea es fundamental reforzar la confianza en los mismos y la base de dicha confianza electrónica está en saber con quién se está interactuando, y tener la certeza de no estar siendo víctimas de fraude. Efectivamente, las estadísticas demuestran que cerca del 70% de los fraudes que se producen actualmente son o están originados en suplantaciones de identidad.

El Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS) estableció el marco para que las interacciones electrónicas entre empresas, ciudadanos y administraciones públicas sean más seguras, más transparentes, más eficientes, sin importar el país europeo en el que se realicen.

Sin embargo, a pesar de los esfuerzos por los Estados Miembros, no se ha conseguido la implantación eficaz de un sistema europeo de identidad digital, fundamentalmente por las discrepancias entre los distintos países, que da lugar a que la identidad digital nacional de cada país no sea interoperable.

Por ello, para eliminar esta barrera electrónica, la Comisión Europea está desarrollando una solución a través de un sistema de identificación europeo (Cartera de Identidad Digital Europea), que viene a subsanar las deficiencias de los sistemas anteriores y ampliar sus beneficios al sector privado.

Efectivamente, a través del Reglamento eIDAS2, se pretende conseguir el acceso de soluciones de identidad altamente seguras y confiables y una aceptación efectiva de los servicios electrónicos de confianza cualificados en la Unión Europea en condiciones de igualdad en cuanto a su prestación.

La Cartera de Identidad Digital va a ser una realidad. De hecho, La Comisión Europea licito en julio de 2022 los servicios de apoyo a la infraestructura de un monedero de identidad digital europeo por 26 millones de €. El objetivo de esta licitación es establecer un contrato marco para desarrollar y aplicar el monedero europeo de identidad digital sobre la base de la propuesta de un marco europeo de identidad digital.

Dicha *Wallet* parte de la base de una aplicación totalmente segura y confiable, creada por entidades que cumplan los requisitos que se marquen por las normas técnicas de aplicación para poder crear las condiciones de confianza precisas. A partir de ahí, cada usuario que instale su *Wallet* tendrá el control exclusivo de su identidad y los atributos que se vayan incorporando a la misma.

La identidad y los atributos que se incorporarán en la *Wallet* estarán emitidos por las entidades correspondientes que puedan certificar que dicha identidad y los atributos son veraces. Estas entidades que emiten y verifican la identidad y los atributos de los usuarios previamente a su incorporación en la *Wallet*, deberán someterse a un proceso de certificación para demostrar su confiabilidad.

Una vez incorporada la información, el usuario podrá elegir con quien compartir estas credenciales.

Los Estados Miembros de la Unión Europea (y entre ellos, España) tienes obligación de proporcionar a sus ciudadanos, a lo largo de 2023, una Cartera Digital confiable, donde se incorpore su identidad digital y los atributos que cada usuario decida.

El objetivo de la Comisión Europea es que, en el año 2030, el 80 % de la población cuente con su sistema de identificación electrónico europeo (e-ID).

11. Protección de datos, seguridad de la información y compliance en los sistemas de gestión integrados o Estructuras de Alto Nivel

Susana González
Manager | Zaragoza - España

En los últimos años, disponer de una estructura de gestión del cumplimiento y prevención de riesgos corporativos se ha convertido en esencial dada la multiplicación y complejidad de las obligaciones de cumplimiento que afectan a las empresas, de todo tipo y tamaño.

De hecho, contamos con normas, de diverso rango y alcance, que establecen obligaciones empresariales de cumplimiento, compromisos éticos, buenas prácticas y de buen gobierno corporativo que exigen a la empresa buena dosis de responsabilidad proactiva en el análisis de sus concretos riesgos de cumplimiento para la definición de controles de prevención, detección y respuesta ante la potencial producción de éstos.

Algunas referencias normativas que están impulsando que, en la actualidad, las empresas tiendan a implantar sistemas de gestión integrados, son las siguientes:

- El artículo 5.2 del Reglamento General de Protección de Datos introdujo el principio de responsabilidad proactiva (*Accountability*) obligando al responsable del tratamiento de datos personales a analizar sus riesgos de privacidad y aplicar las medidas, técnicas y organizativas apropiadas para garantizar - y poder demostrar - el cumplimiento de la normativa de protección de datos personales.

  Es en el análisis concreto de cada empresa cuando se puede definir si está obligada o no a designar un Delegado de Protección de Datos (DPO); configurar un registro de actividades del tratamiento de datos personales; realizar un análisis de riesgos, debiendo documentar los procesos de tratamiento de datos que garanticen la implantación eficaz.

  Es decir, implantar y mantener mediante un proceso de mejora continua, procedimientos e instrucciones que ayuden a que "salten las alarmas" cada vez que se realice un nuevo tratamiento de datos; cada vez que se cree una nueva línea de actividad; o cada vez que se decida utilizar una nueva herramienta tecnológica a través de la que se traten datos personales de los que la empresa sea responsable o encargada del tratamiento. Todo ello con el fin de valorar - y demostrar que se ha valorado - entre otras cosas, si procede o no realizar una evaluación de impacto de privacidad; estructurar el derecho de información a los titulares de los datos; y verificar si las medidas de seguridad existentes son o no las adecuadas al riesgo del concreto tratamiento de datos de que se trate, de cara a garantizar su adecuación con la normativa.

  Vemos aquí presente el enfoque a riesgos en la normativa reguladora del derecho fundamental a la intimidad de las personas desde el punto de vista del tratamiento de sus datos personales por la empresa.

Algo que ha demostrado tajantemente la obsolescencia de la tradicional carpeta en papel con una única y mal denominada "política" repleta de anexos nunca actualizados, ni realmente implantados, por el riesgo que supone: no tener realmente nada.

- Por otra parte, las reformas (2010 y 2015) del art. 31 Bis del Código Penal introdujeron en España la responsabilidad penal de las personas jurídicas por los delitos cometidos, en nombre o por cuenta de estas, y en su beneficio directo o indirecto. Asimismo, se establece como exención si, antes de la comisión del delito, el órgano de administración ha adoptado e implantado de forma eficaz un sistema de gestión que incluya las medidas de gobernanza, supervisión, vigilancia y control (Compliance) idóneas (en virtud de sus concretos riesgos identificados y evaluados) para prevenir o reducir significativamente el riesgo de comisión de delitos.

  Y, por otro lado, se establece como atenuante que la empresa tenga implantadas medidas de control eficaces para prevenir y descubrir infracciones que puedan derivar en ilícito penal. Situación que, generalmente, solventamos con la configuración, regulación y puesta en marcha del canal de denuncias o canal ético.

  En un sistema de gestión de compliance el enfoque a riesgos es claro. Contamos con un catálogo de delitos susceptibles de ser cometidos por la empresa que deben ser diagnosticados. Debe evaluarse el riesgo inherente o intrínseco respecto de cada conducta delictiva constitutiva de cada tipo de delito; deben identificarse los controles existentes en la organización aplicables de forma directa a reducir o minorar cada concreto riesgo; y finalmente, hay que obtener un riesgo residual y un plan para su tratamiento desde el enfoque del proceso de mejora continua.

Los sistemas de gestión de compliance son un "paraguas" por debajo del que prácticamente todo el resto de las medidas preventivas y de diligencia debida actúan como un control en la reducción de los riesgos.

La realidad es que, en un sistema de gestión de riesgos penales, se evalúan riesgos relacionados con el catálogo de potenciales delitos que pueden ser susceptibles de responsabilidad penal de la persona jurídica; sin embargo, generalmente identificamos también riesgos corporativos de otro orden (responsabilidad civil, infracciones administrativas, reputacionales, conflictos laborales, riesgos de seguridad y salud laboral, pérdidas productivas, incumplimiento de contratos, etc.) que a la alta dirección y órgano de administración interesa tener bajo estricto control.

Cuando analizamos un riesgo tan transversal en la totalidad de las empresas actuales como puede ser el riesgo de la comisión de las conductas que constituyen un delito contra la intimidad de las personas; o de daños informáticos; o de descubrimiento y revelación de secretos de empresa; nos encontramos con que, si la empresa ha adaptado todos sus procesos de tratamiento de datos a la normativa de protección de datos, y lo ha implantado de forma eficaz (publicidad y transparencia de la información, formación, análisis, rol y responsabilidad definidos, etc.) supone un control que reduce el riesgo inherente de comisión de la mayor parte de las

conductas delictivas de dichos ilícitos.

Pero es que, a la vez, refuerza la transparencia, la organización, control y buenas prácticas de gobernanza del cumplimiento normativo, en definitiva, liderado por los máximos responsables de la organización.

Compliance es tan transversal que podríamos poner infinitos ejemplos de medidas de diligencia que suponen un control de los riesgos. Así, una empresa que es sujeto obligado por la normativa de prevención de blanqueo de capitales y financiación del terrorismo, si dispone de las medidas de diligencia debida exigidas, debidamente documentadas e implantadas de forma eficaz, conseguirá ver en su mapa de riesgos muy reducido su riesgo inherente, pudiendo así destinar sus recursos a mitigar otros riesgos menos controlados o más críticos.

Si la empresa dispone de un sistema de calidad en el que se regula el proceso de compras y evaluación de proveedores y, en el mismo, bien por cumplimiento de la normativa de prevención de blanqueo, bien por prevención del fraude, corrupción y conflictos de interés, se valora respecto a estos las medidas de diligencia debida que tienen adoptadas relativas a estas cuestiones, ello supondrá un control eficaz para la reducción del riesgo potencial de comisión de conductas inherentes a delitos del tipo estafa, corrupción o tráfico de influencias o fraude a Hacienda o a la Seguridad Social.

Si la empresa dispone de Plan de igualdad aprobado y debidamente implantado, supondrá un control que reduzca el riesgo inherente de un potencial delito de discriminación de trabajadores…

Llegados a este punto, es destacable que, en toda medida de prevención confluye una fase de análisis de riesgo (responsabilidad proactiva) y de documentación, comunicación y formación a personas. Personas trabajadoras, personas usuarias, personas contacto de clientes o proveedores, personas colaboradoras externas, etc. a las que, en cada documento de compromiso, contrato, declaración, formulario o toma de datos de comunicación se debe realizar la debida información sobre el tratamiento de sus datos personales.

De nuevo, vemos aquí un adelanto de las ventajas de la visión integral.

- Por su parte, la Directiva *Whistleblowing*, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, obliga a determinadas empresas a disponer de un canal de denuncias y establecer garantías de protección frente a represalias para las personas que informen sobre irregularidades.

  Disponer de un canal de denuncias eficaz no es montar un formulario web y olvidarnos. La eficacia exige previamente disponer de un **mapa de riesgos** específicos de cada empresa obligada y la implantación de procedimientos reguladores de gestión de dichos riesgos a través de dicho canal como medio de detección; así como la designación de roles y responsabilidades que garanticen el seguimiento de un procedimiento adecuado.

  Las empresas que disponen de sistemas de gestión de compliance

ya disponen de un canal ético o canal de denuncias regulado e implantado; ya tienen definido qué puede denunciarse o qué diferencia una denuncia de una consulta; ya tienen definido el procedimiento para la investigación y resolución de denuncias y designado el rol responsable de ello. Y, algo muy importante, garantizar la no represalia es simultáneo a la implantación de medidas de garantía de la confidencialidad y anonimato.

De nuevo nos encontramos aquí con un resultado de una obligación (el canal de denuncias) que exige el debido análisis e información al denunciante sobre el tratamiento de sus datos personales en todo el ciclo de este.

- La Ley para la igualdad efectiva de mujeres y hombres estableció la obligación de contar con un Protocolo contra el acoso laboral para toda empresa o autónomo que tenga empleados a su cargo, independientemente del número de personas que sean o su volumen de negocio.

Desde entonces, aun cuando no era obligatorio, muchas empresas con más de 250 trabajadores ya implantaron un Plan de Igualdad con el objetivo de ofrecer una imagen transparente responsable y comprometida con la igualdad, o reducir con este control un potencial riesgo de discriminación de trabajadores en sus sistemas de gestión de compliance.

Fue con la entrada en vigor del Real Decreto-Ley de medidas urgentes para garantía de la igualdad de trato y de oportunidades entre mujeres y hombres en el empleo y la ocupación cuando el Plan de Igualdad pasa a ser obligatorio para cualquier organización con más de 50 trabajadores en plantilla (o con menos de 50 trabajadores si lo exige el convenio colectivo aplicable, o cuando se le haya impuesto esta medida en lugar de una sanción por la autoridad laboral competente).

Nos encontramos de nuevo con otra exigencia normativa de cumplimiento que requiere a la empresa el **diagnóstico y análisis**, cuantitativo y cualitativo, para conocer el grado de integración de la igualdad en la empresa; la evaluación y el **desarrollo de políticas de gestión** del personal; la implantación de medidas preventivas y reactivas eficaces y evaluables, y la asignación de roles y responsabilidades para el adecuado seguimiento.

El cumplimiento de la normativa de protección de datos personales vuelve a ser transversal en estos planes, siendo los datos de las personas trabajadoras, datos personales esenciales y habituales en toda empresa.

- Conforme a la Orden por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, para participar en los Fondos *Next Generation* se exige tener debidamente implantado un Plan antifraude, anticorrupción y anti-conflictos de interés; lo que, necesariamente conlleva **evaluar** el estado en el que se encuentra la empresa ante este tipo de potenciales ilícitos; disponer de medidas preventivas de diligencia debida, de detección y correctivas, así como definir los procedimientos e instrucciones adecuados para su seguimiento eficaz.

Huelga decir que, aun cuando hasta ahora la única previsión es que la empresa perceptora de ayudas tenga firmada una declaración responsable de cumplimiento de este requisito, declarar que se dispone de algo que no se tiene, no solo supondría una falsedad, sino que conllevaría el riesgo de que, en fase de justificación, le sea requerido de aportación dicho plan con la trazabilidad del resto de medidas implantadas, so pena de la no concesión final de las ayudas, además de potenciales sanciones.

Gran parte de lo que se exige por esta normativa suele formar parte del habitual procedimiento de medidas de diligencia debida en un sistema de gestión de compliance. En este procedimiento, además de gestionar acciones preventivas sobre entidades bajo control y no controladas, se regulan, implantan y miden medidas de control con otras partes interesadas, básicamente socios de negocio (clientes y proveedores), lo que, de nuevo, suele integrarse con facilidad en los procesos de evaluación previos a la contratación y en la propia contratación.

Nuevamente, tanto en la toma de contacto, como en la evaluación para homologación de un proveedor o alta de un cliente, como en la propia fase de contratación, la información necesaria en torno al tratamiento de los datos personales aparece como mantra transversal.

- Mediante Ley 11/2018 por la que se modifica el Código de Comercio; el Texto Refundido de la Ley de Sociedades de Capital y la Ley de Auditoría de Cuentas, en materia de información no financiera y diversidad, se introduce la obligación de presentar un Informe de Estado de Información No Financiera (EINF), individual o consolidado, a las sociedades que cumplan que, durante dos ejercicios consecutivos, a la fecha de cierre de cada uno de ellos, cumplan al menos dos de las circunstancias siguientes:

    - Que el total de las partidas del activo consolidado sea superior a 20.000.000 euros.
    - Que el importe neto de la cifra anual de negocios consolidada supere los 40.000.000 euros.
    - Que el número medio de trabajadores empleados durante el ejercicio sea superior a 250.

El contenido del informe de EINF debe incluir la información sobre los procedimientos utilizados en la empresa para **detectar y evaluar los riesgos** y el desarrollo de políticas, procedimientos e instrucciones e indicadores sobre cuestiones medioambientales, sociales, laborales, relacionadas con los derechos humanos, relativas a las medidas adoptadas para prevenir la corrupción y el soborno y para luchar contra el blanqueo de capitales.

Para llegar a configurar dicho informe es esencial que la empresa cuente con todos los requisitos debidamente documentados y estructurados y con los consecuentes análisis de riesgos en cada materia y estructura de documentación que evidencie su plena implantación y conocimiento.

¿Qué sucede en estos casos? Nos hemos encontrado con empresas jóvenes con un alto crecimiento en los últimos años obligadas a incorporar este informe en su informe de gestión y que, por el

contrario, no tenían prácticamente nada regulado en casi ninguno de los requisitos o los tenían absolutamente dispersos, confusos e incluso contradiciéndose entre sí. El trabajo de empezar desde cero y, generalmente con un plazo perentorio, es ingente.

En otros casos, los mejores, nos encontramos con empresas que disponen de un sistema de calidad, de seguridad de la información y de medioambiente certificados (y, por tanto, con tradición en sus auditorías periódicas, lo que les obliga al mantenimiento de KPIs sobre sus objetivos anuales). Empresas que, además, han cumplido en plazo y mantienen la adecuación en el tratamiento de los datos personales de los que son responsables y de sus relaciones con los encargados del tratamiento; que disponen de un plan de igualdad, etc.

En estos casos, dado que – con carácter previo a la confección del informe - evaluamos las evidencias de cada punto del informe de conformidad con los parámetros del estándar GRI (*Global Reporting Initiative*), prácticamente siempre encontramos controles eficaces implantados que cubran, sin ningún inconveniente, la confección del informe.

- A excepción de las empresas que tienen obligación de cumplir el Esquema Nacional de Seguridad u otra normativa análoga específica por actividades reguladas, el resto de las empresas no tienen obligación – como tal – de disponer de un sistema de gestión de seguridad de la información SGSI (ISO 27000).

  El desarrollo de un SGSI de nuevo supone partir de un **análisis de riesgos** de la situación en la que se encuentra la empresa en cuanto a su entorno de exposición en seguridad física y lógica; así como de la implantación de las medidas técnicas y organizativas previstas en su plan de tratamiento de los riesgos (al menos de los no asumibles).

  Partimos de la base de que la información con la que trabaja una empresa es de diverso orden. Información comercial, know-how, catálogos, moldes, diseños, matrices, clientes, proveedores, marcas …. Y datos personales.

  Las empresas que tan solo tienen adecuado el tratamiento de los datos personales a la normativa mediante la implantación de las medidas técnicas y organizativas adecuadas al tratamiento y nivel de riesgo de cada tipología y proceso de datos, solo tienen – en el mejor de los casos – protegida una parte de la información empresarial, la que trata datos de personas físicas identificadas o identificables.

  Es cierto que los sistemas que soportan los procesos de tratamiento de la información suelen ser comunes en algunas empresas y que, por lo tanto, si aplicamos a todos los sistemas que soportan todos los procesos de información las mismas medidas técnicas que aplicamos a los procesos de información que tratan datos personales, el avance es importante. Sin embargo, aunque estemos cubriendo medidas de protección y de reacción ante una brecha de seguridad con posible fuga de datos, seguramente no estaremos detectando un incidente. Estaremos quizás procurando garantizar la confidencialidad, pero no siempre la disponibilidad, la accesibilidad y la resiliencia de la información.

Estos son solo 7 casos de cambios normativos o incidencias de otro orden que, en los últimos años, han llevado a la empresa a instaurar un enfoque de gestión de los riesgos y estructuración documental de sus procesos de cumplimiento. Sin embargo, hay muchísimas referencias más, sin olvidar aquellas empresas que, por su específica actividad, se hallan también específicamente reguladas en su entorno de gobernanza y cumplimiento.

En los proyectos de consultoría de **gestión de riesgos empresariales** a menudo nos encontramos con empresas que requieren un sistema de gestión de riesgos penales (compliance) con el objetivo de obtener la identificación de sus riesgos más críticos; que necesitan conocer si los controles implantados son realmente eficaces; e incluso establecer otras medidas de prevención y control que les ayude a mitigar los riesgos de incumplimiento y perpetuar su proceso de mejora continua.

Es habitual que las empresas cuenten con un sólido sistema de gestión de calidad certificado (ISO 9001), generalmente con el alcance determinado a sus procesos productivos y, por lo tanto, dejando al margen de dicha gestión otros procesos de negocio no directamente productivos. Por ejemplo, nos podemos encontrar que se evalúan los requisitos de calidad de un proveedor de producto materia prima que se va a incorporar al proceso productivo, pero no un proveedor de servicios informáticos o de otro tipo de servicios.

Nos podemos encontrar con que la empresa cuente incluso con un sistema de gestión de medioambiente (ISO 14001). En estos casos, lo habitual es que ambos se hallen ya integrados en una estructura de alto nivel (*High Level Structure, HLS*).

En tales casos, ya sea que trabajemos la adecuación de sus procesos de tratamiento de datos personales, o bien de cumplimiento corporativo (compliance), o de seguridad de la información, se nos solicita la más que necesaria integración con el sistema de gestión integral (SIG) de que la empresa dispone.

La mayoría de las normas ISO de sistemas de gestión comparten metodología y algunos requisitos comunes y otros muy específicos.

La estructura de alto nivel para un sistema integrado prioriza la **orientación al riesgo** que, como hemos visto hasta ahora, es común a todos los sistemas de gestión. Además, tiene como objetivo unificar los requisitos genéricos de todas las normas certificables, enfocando de forma diferenciada solo lo específico de cada una de ellas; evitando así, sobre todo, duplicidad de documentación y contradicciones inoperativas.

La metodología de identificación y valoración de los riesgos para cada sistema de gestión suele ser similar, pero son diversos los requisitos a evaluar. En calidad, podemos medir el nivel de satisfacción de un cliente, o el volumen de devoluciones de un producto determinado; en protección de datos, medimos si se producen tratamientos de datos de categorías especiales, o si se trata de un tratamiento automatizado a gran escala que requiera evaluación de impacto; o en compliance, si potencialmente en la empresa se puede producir una estafa, un fraude a hacienda, o un contrabando en expedición. Por ello, es habitual que el mapa de riesgos y su plan de acción sea específico para cada sistema.

Sin embargo, en el diseño de las medidas organizativas de prevención y control existen normas internas que son comunes a todos ellos y, perfectamente, pueden integrarse sin duplicarse, bastando su actualización, integración y referencia.

- Así, si la empresa ya dispone, por ejemplo, de la definición del contexto de la organización y

definición de partes interesadas (*stakeholders*) en su sistema de calidad, no debemos duplicar esta información en el desarrollo de otra normativa interna. Sin embargo, siendo comunes las partes interesadas, sí tendremos que integrar las diversas expectativas de estas en cada sistema de gestión.

Es decir, si "usuarios web" se define en el sistema integrado como parte interesada, su expectativa en el sistema de calidad podrá ser la satisfacción con el producto; en gestión del tratamiento de datos personales, será el cumplimiento de la obligación de información sobre el tratamiento y respuesta al ejercicio de derechos; en compliance, podrá ser la transparencia y buenas prácticas en las condiciones generales de contratación; y en seguridad de la información, la implantación de medidas de seguridad que impidan acceso autorizado a su perfil, la información sobre posibles respuestas ante un incidente, etc.

En estos casos, tomaremos el documento en el que en el sistema integrado (suele ser política o manual, normas de primer nivel) se definan las expectativas e incluiremos las que definamos como propias en cada sistema de gestión a cada parte interesada ya definida.

- Si la empresa ya dispone de un procedimiento de información documentada en el que se defina la codificación de los documentos para un control riguroso de toda la documentación integrada, y defina además quién los crea, quién los aprueba, quién los audita, etc.; no es preciso que se cree un nuevo procedimiento de información documentada para cada sistema, ya que corremos el riesgo de duplicidad o, en el peor de los escenarios, de contradicción.

- Si la empresa ya cuenta con un procedimiento de formación, comunicación y sensibilización en su sistema integrado y, tanto en protección de datos, como en seguridad de la información, como en compliance es requisito formar al personal y sensibilizarle de forma recurrente, no será necesario crear un procedimiento sobre ello para cada sistema, bastando que se incluya en el existente las materias sobre las que se debe formar, su periodicidad y el plan de formación de la empresa.

- Si la empresa en su procedimiento de compras ya dispone de una instrucción y de los formatos o registros correspondientes para la evaluación de los proveedores, de nada le sirve que introduzcamos cláusulas de información del tratamiento de datos de los contactos de proveedores en, por ejemplo, un "Anexo denominado pedido" de un manual de protección de datos de 120 folios, si no les identificamos, con claridad, la concreta instrucción y formatos que modificar del sistema integrado. Debemos concretamente indicar qué cláusula informativa debe incluirse en el formato pedido.

- Si, colgando del mismo procedimiento de compras, existe una instrucción de evaluación de proveedores o de clientes (socios de negocio) será en ésta y en los formatos que cuelguen de dicha instrucción, en los que deberemos ayudar a la empresa a integrar la información sobre el tratamiento de datos personales a clientes y proveedores; las declaraciones responsables a solicitar en materia de prevención del fraude, anticorrupción y anti-conflictos de interés; la solicitud de documentación identificativa, de titularidad real y de titularidad de cuentas bancarias en prevención de blanqueo de capitales, etc.

- Si la empresa ya tiene definido su plan de auditorías y estamos integrando otro sistema de gestión que requiere igualmente auditorías internas y de certificación, bastará con integrarlo en el propio procedimiento de auditoría, en lugar de crear tantos procedimientos de auditoría como sistemas de gestión. Eso sí, la integración deberá siempre incluir las cuestiones específicas, como podría ser en este caso, el diverso perfil a exigir al auditor conforme a los requisitos de cada sistema de gestión.

Como vemos, con la integración de los sistemas de gestión conseguimos, como valor añadido, poner a disposición de la empresa un enfoque común a todos sus sistemas de gestión, con una organización y estructura lógica que facilita la evidencia de buen gobierno y la transparencia ante cualquier inspección o auditoría y la actualización ágil de todos los procesos documentados, en seguimiento de otro de los requisitos más esenciales: la **mejora continua**.

12. Chatbots, asistentes virtuales y su impacto en la privacidad

Salvador Silvestre
Socio | Valencia - España

Uno de los principales retos a los que nos enfrentaremos a lo largo de este año 2023 en el ámbito de la privacidad y protección de datos, será el aumento considerable de asistentes virtuales y *Chatbots* que de un tiempo a esta parte han venido integrándose en la vida de las corporaciones y los ciudadanos.

La irrupción reciente de 'Chat GPT', un chat con Inteligencia Artificial (IA) que está sorprendiendo a todos, quizá haya puesto el foco en el cambio que desde años se está produciendo en el ámbito conversacional. Se trata de un sistema de chat basado en el modelo de lenguaje de IA GPT-3 y genera respuestas muy exactas sin perjuicio de que es muy posible que cometa errores y de facto, en un "*paper*" publicado el 16 de diciembre de 2022 por investigadores de la Universidad de Stanford concluía que el código es más inseguro cuando los programadores se confiaban en los asistentes de IA.

En cualquier caso, más allá de las tremendas expectativas que estos sistemas están despertando en la sociedad, desde un punto de vista legal, debemos apostar porque la seguridad jurídica en el ámbito de la privacidad sea condición esencial para el desarrollo de estos asistentes que cada vez más se integran en la vida personal de los usuarios.

El uso de asistentes virtuales y *Chatbots*, sobre todo si estos integran IA, impactan de forma muy clara en la privacidad de los usuarios. Los datos recabados por parte de los asistentes o el *Chatbot* pueden ser de muy diversa índole y tipología, conllevando en la gran mayoría de ocasiones, que dichos datos tengan la consideración de datos de carácter personal.

Los responsables de tratamiento que vayan a realizar actividades de tratamiento con datos personales, en este caso, a partir de un asistente virtual o *Chatbot*, deberán analizar los riesgos para los derechos y libertades de los usuarios y establecer procedimientos de control que garanticen cumplir los principios de protección de datos desde el diseño y por defecto, pudiendo tener como referencia orientativa la Guía de la Agencia Española de Protección de Datos que aborda estas cuestiones.

Análisis de riesgos y, con toda seguridad en la mayoría de los casos, la realización de una EIPD (Evaluación de Impacto en Protección de Datos) serán herramientas fundamentales para definir y establecer medidas de control y seguridad que se debe realizar por el responsable de acuerdo con las particularidades de las actividades de tratamiento.

13. *Cookieless* y tendencias en sector publicidad digital

Teresa Pereyra
Socia | Madrid - España

El sector de la publicidad digital promete ser uno de los temas tendencia de este 2023. En 2022, la sanción de la Autoridad de Protección de Datos Belga al Interactive Advertising Bureau (IAB) por incumplir el Reglamento General de Protección de Datos (RGPD) a través de su nuevo Marco de Transparencia y Consentimiento hizo tambalear en Europa las bases sobre las que durante años se ha asentado la publicidad digital, provocando la puesta en marcha de diversas iniciativas cuyo objetivo es encontrar alternativas que permitan a la industria seguir ofreciendo publicidad personalizada a los usuarios sin vulnerar el RGPD.

En este sentido, uno de los principales agentes afectados, Google, anunció el lanzamiento en 2024 de un nuevo modelo de navegación sin cookies de terceros.

Por su parte, Vodafone y Deutsche Telecom han estado probando un nuevo sistema de identificación para la publicidad digital, TrustPid, también conocida como la "*supercookie*" que rastrea los hábitos de navegación del usuario mediante la creación de un perfil seudonimizado, creado a partir de un token que funciona a nivel proveedor de servicios. Al proyecto se han unido recientemente Orange y Telefónica, con quienes hay intención de formar una *joint-venture* cuya autorización está pendiente de aprobación por la Comisión Europea. A través de esta, se planea la puesta en marcha oficial de este sistema de rastreo seudonimizado.

Por su parte, el Supervisor Europeo de Protección de Datos, acaba de publicar el informe de conclusiones del grupo de trabajo sobre cookies, en el que dieciocho autoridades de protección de datos han analizado las cuestiones de fondo contenidas en el aluvión de denuncias plantadas por la asociación de Max Schrems, *None of Your Business*. Estas conclusiones, no tienen el carácter de directrices para las autoridades de control, pero si pretenden sentar las bases de unos criterios decisorios coherentes por parte de las distintas autoridades que deberán, en cada, analizar el supuesto de hecho concreto y adaptarlo a la normativa local.

Por su parte, la IAB, tras la sanción recibida en Bélgica presentó un plan de acción con una batería de medidas para remediar las deficiencias identificadas en su Marco de Transparencia y Consentimiento, que ha sido valorado de forma positiva por la Autoridad de Protección de Datos Belga. No obstante, se encuentra pendiente de la decisión del Tribunal de Justicia de la Unión Europea (TJUE) a quien la Autoridad de Protección de Datos ha elevado varias cuestiones prejudiciales de las que depende la validez de su plan.

14. eHealth o salud digital y su impacto en la privacidad

Vanesa Alarcón
Socia | Barcelona - España

En un entorno como en el que vivimos, hiperconectado y no solo debido a ello, pero en gran parte, muy promovido por la situación de pandemia que hemos estado viviendo, han aparecido y están apareciendo, cada vez más, soluciones digitales que pretenden contribuir o prestar servicios en el entorno de la salud o la investigación.

De este modo, han surgido y están surgiendo nuevas iniciativas que utilizan la tecnología para prestar nuevos servicios y/u ofrecer nuevas formas de prestar servicios. En algunas ocasiones, surgen desde startups donde los fundadores han tenido o tienen algún vínculo con el mundo de la salud o la investigación y, en otras, surgen desde empresas u organizaciones con trayectoria en el mercado que promueven el desarrollo de este tipo de iniciativas o proyectos, como una línea nueva de negocio o un complemento a las ya existentes. En algunas ocasiones como, por ejemplo, en el caso de universidades y escuelas de negocios, se promueve la creación de *spin off* derivadas de proyectos con origen en la propia universidad.
Así, solo con mirar las noticias en los diferentes medios, vemos cómo se anuncian servicios tanto de prevención de salud, como de acompañamiento o atención de la salud de forma periódica, como formación en estos ámbitos y algunos proyectos más disruptivos que podrán utilizar incluso tecnologías más sofisticadas como la inteligencia artificial y el *Big Data*, las tokenizaciones, la aplicación de tecnología conectada o el *Internet of things* o incluso proyectos vinculados o enfocados para el mundo del Metaverso.

Algunos ejemplos, por ser más concretos, los podemos encontrar en plataformas que ofrecen servicios de atención psicológica online, dispositivos inteligentes o *Smart devices* conectados que permiten monitorizar los pasos y ejercicio que una persona realiza cada día, entre muchos otros aspectos; otras que ofrecen la monitorización de lo que un usuario come para controlar su dieta o peso; e incluso empresas que analizan tu salud, como las intolerancias alimentarias o el ADN. Incluso están apareciendo herramientas o soluciones para acompañar a los usuarios o pacientes en su día a día, mediante asistentes virtuales.

Lo cierto es que el futuro más próximo se parece, cada vez más, a lo que ya anticiparon películas como *Gattaca* en 1997, *Her* (2013) o incluso la española *Eva*, de 2011. En todas ellas nos podíamos, en cierto modo, anticipar al futuro y ver posibles situaciones y consecuencias de la aplicación de la tecnología a nuestras vidas y a nuestra salud física o mental.

¿Y qué riesgos presentan estas soluciones para la privacidad o la protección de datos personales?

Pues el riesgo empieza desde el momento en que se recoge un dato de salud. La información de salud tiene la consideración de categoría especial de datos según lo dispuesto en el Reglamento Europeo de Protección de Datos de carácter personal o RGPD. Ello es así porque el dato de salud es una información muy personal del usuario, sensible y que, por ello, debe ser especialmente protegida. Su tratamiento por fuera de la ley puede conllevar grandes riesgos para la persona desde un punto de vista de privacidad o intimidad, entre otros derechos que pudieran resultar afectados.

En consecuencia, cuando una empresa tiene la intención de desarrollar proyectos de este tipo, debería proceder a la realización de un análisis sobre el impacto de la privacidad de su proyecto en el usuario, en su vida, determinando de entrada qué es lo que se puede hacer; lo que no, de acuerdo con la ley, porque no sea pertinente no proporcionado o se trate de un tratamiento abusivo y, a partir de ahí, acabar de diseñar la herramienta. A este análisis de privacidad lo llamamos *Data Protection Impact Assessment (DPIA)* o Evaluación de Impacto en la protección de datos (EIPD).

Pero esto no es todo. No solo debemos diseñar desde el inicio de un proyecto lo que podemos o no podemos hacer y cómo pretendemos llevarlo a cabo, sino que también debemos diseñar los pasos para informar al usuario acerca del uso y fines del tratamiento de sus datos de salud y solicitar su consentimiento, disponiendo, también, de adecuados procedimientos, protocolos y medidas de seguridad internas que controlen y custodien adecuadamente esa información sensible.

Para poner un ejemplo, si una empresa o centro de salud desarrolla y dispone de una aplicación de salud para monitorizar o dar seguimiento sobre un tratamiento que recibe un paciente o usuario, como complemento de la prestación asistencial que el paciente recibe, la empresa en cuestión deberá realizar este análisis, para ir bien, de inicio. Todo ello, para controlar que el tipo de información que recaba del usuario es la adecuada y lógica y, en su defecto, corregir, antes de su desarrollo informático; y establecer cómo debe ser el circuito de recogida de datos y uso de esos datos, incluso antes de empezar.

Con ello, se minimiza el riesgo para la privacidad del usuario, por un lado y, por parte de la compañía o entidad, por otro lado, minimizamos el riesgo de sanciones que nos pudiera llegar a imponer la Agencia Española de Protección de Datos (AEPD) por una posible infracción en esa prestación de servicios o tratamiento de datos.

Junto a ello y siguiendo con el ejemplo, se deberá informar al usuario que utilice esa herramienta mediante las condiciones del servicio o términos y condiciones y la correspondiente política de privacidad que incluya el aviso u hoja informativos y de recogida del consentimiento o cualquier otra base de legitimación aplicable. Y ello requerirá de un adecuado circuito de validación del consentimiento, en su caso, además de tener en cuenta otros sistemas de monitorización, en su caso, del usuario, mediante la plataforma puesto que, en función del sistema, si aquel utiliza cookies, deberemos añadir, también, la correspondiente política de cookies.

Y eso no es todo. Como decíamos, si en dicha herramienta recogemos datos, indicamos al usuario que aplicamos las medidas de seguridad y garantizamos su ejercicio de derechos de protección de datos, internamente, debemos tener todas las políticas y medidas que acrediten que ello es así (por ejemplo, aparte de disponer de medidas de seguridad informática aplicadas a la custodia o almacenamiento de los datos, entre otras, disponer de manuales de buenas prácticas para empleados que informen sobre lo que sí pueden realizar o no cuando usan las herramientas y soluciones de la empresa). De lo contrario, podemos incurrir, de nuevo, en riesgo de inspección y/o infracción por parte de la AEPD.

Y en lo que no se suele caer con muchas de estas soluciones es en otros escenarios que también tienen un impacto desde el punto de vista de la privacidad y para el mismo proyecto. Por ejemplo, si disponemos de una solución *eHealth* en formato App con sus correspondientes términos y condiciones, su política de privacidad, pero luego tenemos una *Landing Page* de presentación de la solución, ésta debe tener sus propios

textos legales, esto es, su correspondiente Aviso legal, la Política de Privacidad y la Política de cookies, como mínimo.

Si, además, luego, mediante este tipo de herramientas, aplicamos Inteligencia Artificial o Big Data, el análisis de impacto de privacidad, deberá tener en cuenta estos aspectos y el diseño de la solución también puesto con la aplicación de inteligencia artificial, nos encontramos, en ocasiones, con situaciones de sesgos que pueden llevar a situaciones de discriminación, posibles problemas veracidad de los datos y exactitud, temas de ética que confluyen o se confrontan con la privacidad; o incluso temas de equilibrio y proporcionalidad en el sistema utilizado para aplicar esa inteligencia artificial y realizar perfilados automáticos del usuario, entre muchas otras situaciones. Todo ello sin perjuicio de implementar otro tipo de garantías o salvaguardas adicionales como podría ser, por ejemplo, la intervención del factor humano.

Junto a ello, también hay que analizar muchas otras situaciones relacionadas con el proyecto como dónde se guarda la información y, por ejemplo, si lo realizamos directamente o con un proveedor que tenga sus servidores fuera del espacio europeo porque, en este caso, estaríamos ante una posible transferencia internacional de datos que también habrá que revisar.

Por lo tanto, queda claro que el mundo de la salud digital o *eHealth*, si bien es tendencia, precisa de un buen asesoramiento en el ámbito de la privacidad, también como tendencia, puesto que esta normativa es cada vez más exigente, por cumplimiento normativo, pero también, por ética y respeto a los datos de esos usuarios.

Los proyectos o empresas deben ser conscientes de que el dato es del usuario y que este tiene derecho a conocer y controlar lo que se hace con él, así como que las empresas que lo tratan lo realicen de la forma adecuada.

MADRID

Calle de Serrano, 69
28006 Madrid
T. +34 917 816 160
info@ecija.com

BARCELONA

Av. Diagonal, 458, planta 8ª
08006 Barcelona, España
T. + 34 933 808 255
info.barcelona@ecija.com

ISLAS CANARIAS

Agustín Millares 16
35001 Las Palmas de Gran Canaria
T. +34 928 337 404
Calle Viera y Clavijo, nº 62
38004, Santa Cruz de Tenerife
Teléfono: +34 922 279 901
info@ecija.com

PAMPLONA

Avenida Roncesvalles 4, 1º
31002 Pamplona, Navarra, España
T.: +34 948 40 99 23
info@ecija.com

VALENCIA

Calle Colón nº 15,
Planta 1ª, puerta 1 y 2
46004 Valencia · T +34 960 725 097
info@ecija.com

ZARAGOZA

Calle Colón nº 15,
Planta 1ª, puerta 1 y 2
46004 Valencia · T +34 960 725 097
info@ecija.com