Nuevos análisis en torno a los derechos de autoría e intangibles (artículos de investigación).

Las nuevas obligaciones para la actividad empresarial en el entorno digital: autoridades públicas, nuevos perfiles profesionales y claves para la observancia legal

La actividad económica en un entorno como internet está cada vez más regulada, al menos en territorio europeo, a las normativas ya conocidas como la Directiva de comercio electrónico, la Directiva de la sociedad de la información, la Directiva sobre derechos de autor en el mercado único digital o el Reglamento Europeo de protección de datos, se añaden actualmente las reglas derivadas de la DSA o Reglamento de Servicios Digitales, la DMA o Reglamento de mercados digitales. La Ley para la Europa interoperable, el Reglamento sobre la disponibilidad de los datos y el propio Reglamento Europeo de IA que establece nuevas tareas de supervisión y control, que indudablemente variarán el escenario actual de perfiles profesionales y jurídicos que asisten a las empresas en el entorno digital. Además, se ha acelerado la creación de organismos y autoridades que en cada Estado europeo velarán por el cumplimiento de cada una de las normativas citadas.

En este artículo de investigación examinamos cada una de las nuevas normas, los perfiles jurídicos que regulan y que en breve se aproximarán y las consecuencias para las empresas y entidades que trabajamos en el entorno digital, en definitiva, la serie de obligaciones legales que más pronto o más tarde deberemos cumplir. Sin ánimo de alertar sino de informar y aclarar qué será obligatorio, y como siempre, con espíritu crítico, explicando lo que sucede realmente cuando las normas entran en vigor y son exigibles.

Las recientes normativas europeas nos traen no solo principios, reglas y estándares aplicables a nuestra actividad en internet, sino que regulan hasta 3 tipos de perfiles profesionales, algunos ya conocidos para las empresas aunque con funciones actualizadas, otros nuevos que pronto serán habituales en el ámbito digital:

- La figura del **delegado de protección de datos**
- La figura del **guardián de acceso**;
- La del **alertador de confianza o fiable**;
- La del **supervisor de inteligencia artificial** (IA).

Igualmente, se están creando **organismos públicos** encargados del control y aplicación de las normas europeas, junto a la Agencia Española de Protección de Datos (a quien puede corresponder la labor de **coordinador de datos**):

- El **coordinador de servicios digitales**, organismo público que se crea en cada Estado europeo. En España es la CNMC– Comisión Nacional de los Mercados y la Competencia;
- El organismo **supervisor de IA**, en España, es la AESIA- Agencia Española de Supervisión de IA .

En este artículo de investigación analizamos sus funciones, así como las obligaciones que deberemos cumplir quienes prestemos servicios en internet, grandes plataformas y también todas aquellas empresas que ofrecemos productos y servicios en el entorno digital, aunque el artículo se enfoca en las ventajas que estas normas generen sobre la parte usuaria o consumidora digital, supuestamente, la principal beneficiaria de este conjunto de reglas y normativas.

Si necesitas más información sobre la gestión de intangibles, contacta con la Asociación Intangia

C/ San Julián, 22 31171 Ororbia-Navarra

Teléfonos: 948 321399 619 322 210

Correo electrónico: info@intangia.es

Las normativas europeas aplicables al entorno digital y a prestadores de servicios y contenidos digitales:

El ámbito digital está cada vez más regulado, al menos en territorio europeo. Las políticas europeas (Programa Europa DIGITAL) quieren garantizar un uso amplio y seguro de las tecnologías digitales en la economía y en la sociedad, apoyando y financiando áreas claves (ciberseguridad, supercomputación, IA, competencias digitales avanzadas…) También se centran en las capacidades que necesita la propia ciudadanía para el uso de la tecnología, para ello, se crea la **Declaración de los derechos y principios digitales**, entre los que se encuentran principios como la inclusividad de las tecnologías— que implica el acceso de la conectividad y la educación en habilitades digitales-, la ética y transparencia— en sistemas de IA–, la libertad de elección en línea— bajo un entorno en línea confiable, teniendo en cuenta el papel que deben cumplir las grandes plataformas en línea–, o la privacidad, entre otros.

Los objetivos de la regulación digital son, básicamente, trabajar para que la ciudadanía tenga habilidades digitales y se especialicen profesionales con altas capacidades digitales, conseguir que las infraestructuras digitales sean seguras y estén protegidas, reforzar la transformación digital también en el ámbito de las empresas, y conseguir que los servicios públicos estén digitalizados.

Esta estrategia se traslada al ámbito normativo, se han creado nuevas Directivas y Reglamentos Europeos que no solo generan obligaciones para los prestadores de servicios, y derechos para los usuarios de contenidos y servicios digitales, también ha generado nuevos **perfiles jurídicos,** con nuevas **entidades públicas supervisoras**, y **perfiles profesionales** que asisten a las empresas y entidades que prestan servicios digitales, perfiles, algunos ya viejos conocidos, como el Delegado de protección de datos, con funciones actualizadas, otros de reciente creación, que analizamos a continuación; en la siguiente tabla se indica la nueva norma europea aplicable y el perfil jurídico que regula:

Reglamento de protección de datos	**Delegado de protección de datos**
Reglamento de datos	**Coordinador de datos**
Reglamento interoperabilidad datos	**Coordinador de interoperabilidad**
DSA– Reglamento Europeo	**Coordinador de servicios digitales** **Alertador de confianza**
DMA– Reglamento Europeo	**Guardianes de acceso**
Reglamento de IA	**Supervisor de IA**

(Cuadro 1.Fuente: propia)

Analizamos a continuación cada una de las normativas europeas, los perfiles jurídicos y sus funciones, las obligaciones para las grandes plataformas en línea y los derechos de los que usamos y operamos en estas plataformas, los usuarios. Centramos este estudio en los perfiles que afectarán a empresas y entidades privadas, descartando algunos, como el coordinador de interoperabilidad, que trabaja solo en el sector público.

El perfil profesional derivado de las normativas de protección de datos personales: Delegado de protección de datos y Coordinador de datos

El Reglamento Europeo 2016/679 es el Reglamento General de protección de datos (RGPD), introduce una figura profesional que hoy todos conocemos, la figura del **Delegado de protección de datos**, cuya función principal es la asistencia y el asesoramiento necesarios en el proceso de adopción de medidas para el tratamiento y la protección de los datos personales (art. 39.1. RGPD). Las funciones concretas son:

⇒ Informar y asesorar al responsable del tratamiento de los datos;

⇒ Supervisar, realizando tareas como la evaluación de impacto, documentando los incumplimientos y controlando las situaciones de ejercicios de derechos por parte de los titulares;

⇒ Cooperar con las autoridades, siendo punto de contacto entre estas y los responsables del tratamiento de los datos.

Queda también claro, no solo por parte del RGPD y de los informes de las autoridades nacionales, como en España la Agencia Española de Protección de datos (AEPD), que el Delegado de protección de datos no tiene responsabilidad sobre el cumplimiento del RGPD; así lo han confirmado decisiones como la STJUE en el asunto X-FAB- C-453/21– en el que expresamente se resuelve que esta figura no puede encargarse de determinar los fines y los medios para el tratamiento de los datos personales; o la STJUE del asunto Leishitz– C-534/20– en el que se impone la garantía de la independencia del Delegado de protección de datos.

En 2023 un nuevo informe de la AEPD actualiza las funciones del Delegado de protección de datos (Informe 0038/2023), que valida el puesto del **Delegado de protección de datos y responsable de privacidad**, que puede realizar funciones nuevas como las siguientes:

⇒ Informar, asesorar y crear los procesos de gestión de riesgos para la privacidad

⇒ Realizar evaluaciones de impacto sobre privacidad

⇒ Gestionar, coordinar y controlar los términos y obligaciones de terceros relacionados con la privacidad.

⇒ Realizar auditorías internas y externas relacionadas con la privacidad.

Recordemos que esta figura del Delegado de protección de datos es obligatoria en algunos entornos: por ejemplo en el ámbito de las Administraciones Públicas (aunque ya conocemos la famosa "moratoria" para que las entidades públicas españolas no sean sancionadas cuando incumplen el RGPD), en algunas entidades semi públicas, en entornos empresariales en los que se tratan datos de alto nivel de protección, o datos que se recogen para determinadas finalidades (el análisis comportamental de los usuarios de forma masiva, por ejemplo).

Y en los últimos meses, tras la entrada en vigor del Reglamento 2024/1689, o Reglamento de IA, una de las preguntas que más se repiten es si el Delegado de Protección de datos podría asumir funciones como responsable de IA de una empresa o de una entidad pública. Para responder a esta pregunta, primero explicaremos estos nuevos perfiles jurídicos derivados de esta norma Europea: el responsable de IA, el supervisor de IA, oficial de riesgo de IA (Ai risk officer) o CDO (chief data officer) para responder luego si alguno de estos perfiles profesionales podría asumir funciones relacionadas con la privacidad o la protección de los datos personales.

Esto lo haremos más adelante.

El perfil profesional derivado de las normativas de protección de datos personales: Delegado de protección de datos y Coordinador de datos (continuación)

Otra de las figuras relacionadas con la protección de datos personales es el que han denominado **Coordinador de datos.** Esta figura aparece en una normativa europea reciente, el Reglamento Europeo 2023/2854, el denominado Reglamento de datos (Data Act), que abre un nuevo marco legal para los datos, basado en principios como la accesibilidad, la transparencia y la protección y a la vez promueve un sistema de gestión de los datos más competitivo, para que las empresas aprovechen al máximo el acceso y el uso de los datos.

[El término **dato** tal y como aparece en este Reglamento de datos de 2023, se refiere no solo a datos personales sino también a aquellas informaciones que derivan del uso de productos y servicios, que pueden ser comunicadas a través de comunicaciones electrónicas como redes 2G o 3G, de conexiones físicas o descargarse a través de dispositivos como usb, por ejemplo. Para entender mejor el concepto de dato, aconsejamos la lectura del artículo "*The data act & policy options for a sectoral regulation to protect competition in the Automotive afterwarner*" de Daniel Gill– *más información en referencias bilbiográficas*– en el que se analiza el concepto en un sector económico concreto, el del automóvil, cuyo mercado postventa requiere del acceso a los datos del vehículo y de la interoperabilidad técnica del vehículo para suministrar determinados servicios o productos, como la reparación o el mantenimiento; las empresas que ofrecen estos servicios necesitan el acceso (remoto) a funciones o recursos específicos del propio vehículo, y pueden suponer el acceso a datos personales del usuario del vehículo, o incluso a informaciones protegidas como secretos empresariales, derechos de autor o propiedad industrial].

El uso del dato debe realizarse bajo principios como el principio de accesibilidad, transparencia y no discriminación, interoperabilidad y portabilidad, protección de secretos comerciales, uso ético de los datos (de forma que no puedan ser utilizados para desarrollar productos o servicios que compitan con otros, esto sería un acto de competencia desleal) y también la protección de los datos personales, de forma que deba aplicarse el RGPD tanto en la recogida (informando y recabando el consentimiento) como en el diseño de los productos y servicios, así como aplicando las medidas legales y técnicas de seguridad reguladas en el RGPD.

Para garantizar la aplicación de este Reglamento de datos se otorgan funciones a las autoridades administrativas que operan en el ámbito de la protección de datos, por ejemplo, en España, a la AEPD. Aunque también alude a la creación de una nueva autoridad administrativa en organismos públicos que supervisen la aplicación del Reglamento de datos, en la que opere la nueva figura del **coordinador de datos**, un puesto administrativo que actuará como punto de contacto entre las autoridades públicas encargadas de velar por el cumplimiento de la normativa europea y los usuarios que puedan interponer reclamaciones por vulneración de su derecho fundamental a la protección de sus datos personales. Daniel Gill habla de un **administrador de datos** que se encargue también de un servidor compartido donde se almacenen los datos, para garantizar el acceso y uso bajo estos principios básicos. Si la AEPD en España asume estas funciones derivadas del Reglamento de datos, deberá nombrar a un coordinador de datos.

Es por lo tanto, un perfil del ámbito administrativo, público, y no será obligatorio para las empresas. Lo que sí será obligatorio para las grandes empresas fabricantes de productos conectados, o suministradores de servicios relacionados con estos productos, es el cumplimiento de este Reglamento, a partir del 12-09- 2025.

Por cierto, también se aplica el Reglamento de datos al uso de contratos inteligentes para la ejecución automatizada de los acuerdos de intercambio de datos, regulando los requisitos a cumplir por los proveedores de aplicaciones que utilicen este tipo de contratos inteligentes (ejemplo: proveedores de cripto servicios, blockchain, etc).

El perfil profesional derivado de las normativas reguladoras de los mercados digitales: qué son los guardianes de acceso

En este entorno digital de productos y servicios, el Reglamento Europeo 2022/1925, denominado Reglamento de Mercados Digitales (DMA), regula unos mercados concretos del ámbito digital, entre los que se encuentran los servicios de plataformas, servicios de intermediación como motores de búsqueda (ej: Google), tiendas de aplicaciones como Amazon, plataformas digitales de intercambio de videos o contenidos (Youtube), redes sociales (Meta, Byte Dance), publicidad online, computación en la nube (Apple, Microsoft), navegadores web, sistemas operativos y asistentes virtuales, entre otros [*veremos a continuación qué empresas deben cumplir ya con el Reglamento*].

Estas empresas que están obligadas al cumplimiento son empresas con unos requisitos concretos: prestan servicios digitales, con un volumen de negocio determinado o bien operan en al menos 3 Estados Europeos de forma simultánea, y tienen un nº elevado de usuarios activos permanentes (calculados en los últimos 3 años); la norma europea se aplica a grandes compañías, pero esto no significa que no haya implicaciones para pymes, para profesionales y empresarios autónomos o incluso para los usuarios finales de estos productos o servicios. Vayamos primero a analizar los perfiles jurídicos derivados de este Reglamento europeo y luego analizaremos las implicaciones para usuarios profesionales y finales.

El Reglamento nº 1925 de 2022 regula la figura del **guardián de acceso** ("gatekeeper"), una categoría en la que entran todas aquellas empresas o plataformas que cumplen esos requisitos mencionados. Por lo tanto, guardián de acceso es una gran empresa que ofrece servicios en línea o facilita plataformas o redes sociales, actuando como intermediarias entre otras empresas y los usuarios finales en este entorno digital.

La empresa calificada como guardián de acceso tiene varias obligaciones legales a cumplir:

⇒ Permitir que los usuarios profesionales que usan sus servicios digitales puedan ofrecer o celebrar contratos con los usuarios finales fuera de su servicio o plataforma;

⇒ Permitir que los usuarios finales puedan desinstalar aplicaciones preinstaladas o modificar la configuración de los asistentes virtuales o del navegador web predeterminado por la empresa;

⇒ Permitir que se puedan instalar aplicaciones o tiendas de terceros;

⇒ Proporcionar a los usuarios profesionales información gratuita y en tiempo real acerca de los datos que generan usando el servicio o plataforma, incluyendo datos personales;

⇒ Proporcionar a los usuarios información gratuita y diaria de la publicidad que ofrece, y también del precio que paga el anunciante, o bien el sistema de cálculo de este coste de publicidad o el pago que recibe el editor;

⇒ Garantizar que las plataformas más pequeñas puedan usar servicios de mensajería de su empresa o plataforma, garantizando la interoperabilidad;

⇒ Permitir que los usuarios, sean profesionales o finales, puedan reclamar por incumplimiento de obligaciones de la empresa que ofrece el servicio o la plataforma;

⇒ Garantizar que no se aplican condiciones contractuales idénticas en el servicio o plataforma a todos los usuarios profesionales;

⇒ No obligar a usuarios profesionales a contratar servicios complementarios o accesorios por usar el servicio o plataforma;

⇒ No obligar a los usuarios profesionales a inscribirse a otras plataformas como condición para usar su servicio o plataforma;

⇒ No rastrear a los usuarios finales y su comportamiento fuera del servicio o plataforma propia, si este no ha dado consentimiento efectivo para dicho seguimiento comportamental.

El perfil profesional derivado de las normativas reguladoras de los mercados digitales: qué son los guardianes de acceso (continuación).

Sin duda, estas obligaciones tienen mucho que ver con quienes utilizamos los servicios digitales o plataformas, nos afecta tanto a pymes como a usuarios profesionales y usuarios finales. Pero antes enumeraremos las compañías que ya han sido calificadas como guardianes de acceso.

La Comisión Europea ha designado ya en un informe de 6 de septiembre de 2023 a varias empresas como guardianes de acceso: Alphabet (matriz de Google), Amazon, Apple, Bytedance (responsable de Tik Tok), Meta (responsable de Facebook, Instragram y Wathsapp) y Microsoft. Y en 2024 a Booking y a X (el enlace a los documentos de designación está a vuestra disposición en *referencias bibliográficas*). A continuación un breve ejemplo de algunas de las obligaciones que deben cumplir:

⇒ El navegador Google Chrome tiene la obligación de facilitar el cambio de motor de búsqueda en cualquier aplicación Android

⇒ Amazon debe recabar el consentimiento expreso para que los usuarios de sus servicios (Amazon Prime, Twich) reciban publicidad personalizada

⇒ Apple debe proporcionar la posibilidad de instalar un sistema operativo diferente

⇒ Bytedance debe facilitar la portabilidad de datos de los usuarios de Tik Tok a otras plataformas

⇒ Meta tiene la obligación de mejorar la portabilidad de datos de sus plataformas y sistemas de mensajería (Wathsapp) para que los usuarios puedan recibir mensajes a través de sistemas de mensajería de terceros

⇒ Microsoft debe facilitar que los usuarios desactiven su sistema de búsqueda Bing , o que usuarios de su sistema operativo Windows puedan desinstalar aplicaciones (cámara de fotos, etc) para instalar las de terceros

Una cuestión importante de esta normativa es que estas obligaciones pueden aplicarse tanto a usuarios profesionales que utilizan estos servicios y productos digitales como a usuarios finales. Un **usuario profesional** es aquel que utiliza estos productos y servicios digitales para su actividad económica (ej: la empresa que vende en Amazon es un usuario profesional de la plataforma); para los usuarios profesionales, los **guardianes de acceso** tienen la obligación de contribuir al crecimiento y no poner trabas con el uso de los servicios digitales: por ejemplo, tienen la obligación de facilitarles si deciden cambiar de plataforma de venta, se les prohíbe aplicar en las condiciones de contratación obligaciones como la contratación de servicios o productos accesorios, o están obligados a permitir que el usuario profesional envíe publicidad de sus propios productos o servicios directamente a los usuarios finales.

Un **usuario final**, aquel que es el consumidor final de los productos o servicios digitales, sigue teniendo los derechos que aparecen en el RGPD, como titular de los datos personales que son tratados por los **guardianes de acceso**, deberá prestar su consentimiento informado para que utilicen esos datos personales de forma cruzada o combinada con otros servicios que ofrece el guardián de acceso, para ceder esos datos a terceros proveedores del guardián de acceso o para recibir anuncios personalizados.

Por lo tanto, tanto usuarios profesionales como usuarios finales podemos ejercer varios derechos frente a las grandes empresas tecnológicas ya designadas como guardianes de acceso. La propia Comisión Europea tendrá competencias en el seguimiento del Reglamento Europeo, competencias inspectoras y de atención a los usuarios profesionales y finales, que podremos informar a las autoridades nacionales o a la propia Comisión sobre las actividades de los guardianes de acceso. Los usuarios tendremos entonces capacidad de control a estas empresas.

El perfil profesional derivado de las normativas reguladoras de los contenidos y servicios digitales: qué es un coordinador de servicios digitales y el alertador de confianza

Otra normativa a analizar es el Reglamento Europeo 2022/2065, el denominado Reglamento de Servicios Digitales (DSA). Esta norma de aplicación directa se aplica a servicios del entorno digital, con el objetivo de garantizar un entorno en línea seguro, permite actuar contra actividades ilícitas o nocivas, o incluso contra la desinformación. Los principales obligados a su cumplimiento son los **servicios de intermediación en línea,** como por ejemplo, los motores de búsqueda, las plataformas digitales, los servicios de alojamiento de datos, los proveedores de acceso a internet, de alojamiento web o de registro de dominios. Para dicho cumplimiento, primero debe cumplirse el siguiente requisito: que la Comisión Europea haya designado a estas empresas como obligadas al cumplimiento. Entre las empresas obligadas al cumplimiento de la DSA están, por supuesto, las plataformas en línea de gran tamaño y los motores de búsqueda de gran tamaño (todos ellos si tienen más de 45 millones de usuarios europeos): Amazon, Google (con servicios como el buscados pero también Youtube), Meta (empresa que gestiona Facebook, Instagram), aunque también aparecen otras como Booking, Pinterest, Zalando… [el listado actualizado se puede ver en el enlace que se facilita en *referencias bibliográficas*].

Las principales obligaciones son las siguientes:

⇒ La creación de un punto de contacto para los usuarios y las autoridades que controlan el cumplimiento de la DSA, así como un canal de denuncias de posibles actuaciones ilícitas dentro de sus servicios digitales;

⇒ La redacción de unas condiciones y términos de uso fácilmente accesibles, fáciles de lectura, transparentes, que establezcan las normas de uso de la plataforma o motor de búsqueda; dicha transparencia se lex exige también en relación a la publicidad, los sistemas de moderación de contenidos que aplican o las recomendaciones a los usuarios;

⇒ La realización de la evaluación de riesgos derivados del servicio digital que ofrecen, en especial en relación a los contenidos ilícitos, en relación al ejercicio de derechos fundamentales (libertad de expresión e información, protección de datos personales, protección de consumidores, derechos de los menores) o sobre contenidos relacionados con procesos electorales, etc. Esta evaluación de riesgos servirá para adoptar medidas que disminuyan o eliminen esos riesgos, para realizar una auditoría anual y para redactar los informes que luego deben enviar a las autoridades europeas. También permitirá que determinados grupos de investigación puedan acceder a los datos de la plataforma para detectar riesgos sistémicos.

⇒ En relación a los datos de los usuarios, se imponen medidas como dar la opción de que el sistema de recomendación de contenidos no se base en los perfiles de los usuarios, o que tengan que crear un repositorio de anuncios que pondrán a disposición del público

El seguimiento de la DSA se realiza por el **Comité Europeo de Servicios Digitales**, órgano europeo que lleva desde febrero de este año 2024 coordinando y supervisando la aplicación de la DSA. Este es un órgano administrativo dependiente de la propia Comisión Europea, y bajo su presidencia, reúne a los coordinadores de servicios digitales nombrados en cada uno de los estados europeos. Por lo tanto, el primero de los perfiles que crea esta norma es el **coordinador de servicios digitales**, que ayudan a la Comisión Europea a hacer cumplir este Reglamento Europeo. Cada Estado miembro debe nombrar a un organismo público que trabaje como coordinador de servicios digitales. En España el organismo encargado es la Comisión Nacional de Mercados y Competencia (CNMC).

El perfil profesional derivado de las normativas reguladoras de los contenidos y servicios digitales: qué es un coordinador de servicios digitales y el alertador de confianza (continuación)

El **coordinador de servicios digitales** es entonces un organismo público estatal que supervisa el cumplimiento de la DSA dentro de cada estado europeo. En España la CNMC tendrá funciones además de control a las plataformas digitales, pueden solicitarles el acceso a los informes y datos derivados de la evaluación de riesgos, incluso tienen capacidad sancionadora, en caso de incumplimiento de la DSA. En relación a los usuarios de las plataformas y servicios digitales, pueden denunciar directamente ante la CNMC cualquier infracción que hayan detectado durante el uso de la plataforma, incluyendo, por ejemplo, infracciones contra contenidos protegidos por la legislación de propiedad intelectual.

Tienen también dos funciones de lo más interesantes:

⇒ Certificar a los alertadores de confianza;

⇒ Certificar a los posibles órganos extrajudiciales de resolución de conflictos que puedan intervenir en el caso en que el usuario haya decidido interponer una reclamación contra las plataformas digitales por esta vía;

En relación a la intervención de entidades alternativas de resolución de conflictos, esto no es nada nuevo, ya desde la Directiva de comercio electrónico (Directiva 2000/31/CE) se ha impulsado la resolución extrajudicial de conflictos relacionados con el consumo en línea.

Lo novedoso es la figura del **alertador de confianza**, un perfil jurídico que aparece por primera vez en la DSA (se habla de alertador o denunciante de confianza, o alertador fiable), perfil nombrado por el coordinador de servicios digitales para detectar, identificar y notificar contenidos ilegales. El alertador de confianza ("trusted plaggers") debe ser un organismo independiente que tenga experiencia en la detección, identificación y eliminación de contenidos ilegales en línea; por supuesto, pueden ser organizaciones de la sociedad civil, siempre que cumplan estos requisitos (art. 22 DSA):

⇒ Experiencia y competencia

⇒ Independencia

⇒ Diligencia, precisión y objetividad

En el caso en que el alertador de confianza, certificado, detecte un contenido ilegal, deberá notificarlo a las plataformas en línea, que deberán atender de forma prioritaria este requerimiento. Anualmente, el alertador de confianza deberá emitir un informe detallado, siempre bajo parámetros de transparencia y facilidad de lectura, que recoja las notificaciones que han enviado a las plataformas digitales, los tipos de contenidos ilegales detectados y las medidas que han adoptado las plataformas al recibir estas notificaciones.

La Comisión Europea dispone de un listado de alertadores de confianza (el enlace en *referencias bibliográficas*), entre los que se encuentran la CIARC– Centro de información sobre derechos de autor y antipiratería de Finlandia.

La pregunta a continuación es si podrían ser alertadores de confianza las entidades de gestión de derechos de autor y derechos conexos que operan en Europa En relación al cumplimiento de los requisitos, está claro que tienen experiencia en detectar contenidos ilícitos (si se trata de contenidos no autorizados por los titulares de derechos para su publicación en línea). La independencia respecto a las plataformas digitales se puede analizar. La diligencia y objetividad me temo que dependerá de la organización interna y la forma de actuación de cada entidad gestora.

El perfil profesional derivado de la normativa reguladora de sistemas de IA: el supervisor de IA, funciones y problemática

Una última normativa a analizar, muy reciente además, es el Reglamento 2024/1689, el Reglamento de inteligencia artificial (IA act). Para la aprobación y la correcta supervisión en la aplicación del Reglamento de IA se han creado algunos organismos públicos europeos: el Consejo Europeo de IA, la Oficina Europea de IA y el Foro Consultivo. La Oficina Europea de IA a su vez realizará esta supervisión a través de las autoridades nacionales, las agencias estatales de supervisión de IA, que en España se llama AESIA, (organismo público estatal con sede en A Coruña) que tendrán las siguientes funciones principales:

⇒ Supervisar los sistemas de IA de alto riesgo que se implanten en cada territorio europeo

⇒ Crear estándares y buenas prácticas para aplicar a sistemas de IA

⇒ Coordinar cualquier tarea de control con otras autoridades de vigilancia del mercado (por ejemplo, la CNMC)

⇒ Evaluar los sistemas de IA

La Agencia AESIA dispone ya de un estatuto, aprobado por Real Decreto 729/2023 de 22 de agosto, que regula sus competencias y funcionamiento, que deben ser conformes a la regulación del Reglamento Europeo de IA; como la norma europea se ha aprobado con posterioridad a la española, debe producirse una adaptación de las funciones de AESIA en los próximos 2 años a dicho Reglamento europeo. Por ejemplo, en el Reglamento de IA, y no en el régimen de funcionamiento de la agencia española de supervisión de IA, aparecen varias definiciones de agentes o intervinientes en cualquier sistema de IA que también pueden servir para determinar los **perfiles jurídicos** que están implicados en el desarrollo por un lado y uso o explotación por otro, de sistemas de IA. Veamos cuales son:

⇒ Se describe en primer lugar al **proveedor de sistemas de IA,** como la persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente; el proveedor deberá cumplir con el Reglamento de IA si lo quiere comercializar en territorio europeo; un ejemplo es OpenAI, que ha desarrollado ChatGPT;

⇒ Aparece también la figura del **responsable de despliegue**, la persona física o jurídica, autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, en el ámbito profesional o empresarial; si lo usa para una actividad no profesional, o actividad personal, no se le califica como responsable del despliegue; un ejemplo es Adobe, empresa que ha incorporado ChatGPT, a través de una marca propia, Adobe Firefly, en su editor de video Premiere Pro, para agilizar procesos en la edición de películas de cine; a esta figura también se le puede denominar **implementador**, ya que se puede encargar de buscar soluciones técnicas basadas en IA en un entorno empresarial concreto;

⇒ La tercera figura o perfil jurídico es el **representante autorizado**, la persona física o jurídica que haya sido designado por un proveedor de IA que no está establecido en el territorio europeo; el representante autorizado sí debe tener establecimiento en la UE, y cumplirá en nombre del proveedor las obligaciones derivadas del Reglamento. Entre proveedor y representante debe existir un contrato de mandato escrito. Como OpenAI tiene residencia en Irlanda, Europa, no estará obligada a designar un representante autorizado.

El perfil profesional derivado de la normativa reguladora de sistemas de IA: el supervisor de IA, funciones y problemática (continuación)

⇒ Otra figura es el **importador**, la persona física o jurídica que comercializa un sistema de IA en la UE y no se trata ni del proveedor ni del responsable del despliegue, ya que lo importa bajo la marca del proveedor establecido fuera de la UE;

⇒ La figura del **distribuidor**, por su parte, es quien comercialice un sistema de IA en territorio europeo y no se trate ni de proveedor ni de importador

⇒ La figura del **proveedor posterior**, es quien comercializa un sistema de IA que incorpora un modelo de IA general, ya se trate de un modelo de IA posterior propio o de un tercero.

Todos ellos pueden ser calificados como operadores de sistemas de IA. Cualquiera de estos perfiles pueden estar obligados a cumplir con algunas normas derivadas del Reglamento de IA, aunque la normativa establece obligaciones concretas para empresas desarrolladoras de IA que no tengan sede social en Europa: **nombrar un representante autorizado con establecimiento en la UE**, antes de la comercialización de sistemas de IA de alto riesgo; este perfil debe cumplir las mismas funciones que un proveedor o un implementador: redactar una declaración de conformidad, registrar los sistemas de IA de alto riesgo, conservar durante 10 años cualquiera de estos documentos, o ser punto de contacto con las autoridades nacionales y europeas.

Ya se exige este perfil en la comercialización de productos como maquinaria y equipos industriales, productos electrónicos, juguetes, sustancias químicas, cosméticos, por lo que no es un perfil nuevo, pero en el ámbito de los sistemas de IA, se recomienda tener conocimientos expresos y completos sobre las obligaciones derivadas del Reglamento, ya que estará obligado a dicho cumplimiento.

Algunos de estos sistemas de IA de alto riesgo realizan también tratamiento de datos personales; por ejemplo, los **sistemas automatizados de toma de decisiones** (un ejemplo de sistema IA con esta función es FindlyIA, que toma decisiones automatizadas posterior al análisis de datos, y que tiene aplicaciones tanto en el comercio electrónico como en el ámbito sanitario con información del paciente a tiempo real). Por lo tanto, se implican también perfiles como el **Delegado de protección de datos (DPO)**, que como hemos explicado en apartados anteriores, debe realizar una evaluación de impacto de los sistemas automatizados de tratamiento de datos, especialmente si suponen la toma de decisiones automatizadas, para incorporar, desde el diseño o por defecto, salvaguardas legales para la protección de los datos personales, antes incluso del desarrollo o la implementación de estos sistemas de IA. Así lo han confirmado decisiones judiciales como la STJUE del asunto C-634/21 (asunto SCHUFA) que confirma la aplicación del art. 22 del RGPD (Reglamento 2016/679/UE), reforzando la intervención de esta figura del DPO. Para estos casos, volvemos sobre la cuestión planteada antes: si el Delegado de Protección de datos podría asumir funciones como responsable de IA de una empresa o de una entidad pública.

Es muy interesante el informe de CEDPO de julio de 2024 (referencias en *bibliografía*) que contempla varios escenarios, desde el que el DPO sea a su vez **responsable de IA** de una empresa (en pymes que no puedan recurrir económicamente a dos perfiles legales contratados, hasta el que contempla un perfil de DPO y otro de responsable de IA, por ejemplo, en grandes compañías. En cualquier caso, los DPO tendrán más funciones para garantizar que el sistema de IA cumpla con la normativa de protección de datos personales, incluso, la CEDPO se plantea crear un perfil, el "**oficial de riesgo de IA"** (AI risk officer) para controlar el riesgo, que es el principal objetivo del Rgto. IA. También afectará al CDO (Chief Data Officer) o director de datos, aunque este es un perfil más técnico.

Los derechos de los usuarios digitales: ventajas e inconvenientes

Las normativas analizadas regulan también los **derechos de las personas usuarias** de los contenidos y servicios digitales; resumimos a continuación los principales derechos de los usuarios ante las empresas que ofrecen contenidos y servicios digitales regulados por las normativas anteriores:

⇒ Los derechos recogidos en la normativa de protección de datos personales se siguen aplicando: el derecho de acceso para conocer la información personal que disponen, rectificación para cambiar datos erróneos o no actualizados, oposición para manifestar el desacuerdo con el tratamiento de los datos, supresión o ejercicio del derecho al olvido ante los sistemas de búsqueda por internet, limitación del tratamiento a los datos que sean solo necesarios, así como la portabilidad de los datos personales de una plataforma o servicio a otro que hayamos elegido;

⇒ El derecho a tener información sobre el tratamiento de nuestros datos personales, sobre los contenidos o servicios que ofrecen los prestadores de servicios en internet, sobre quién es la empresa o entidad responsable, sobre el precio de los servicios o contenidos en su caso;

⇒ El derecho a ser informados también sobre el uso de sistemas de IA y de tener acceso a todos los documentos que exige el Reglamento de IA: declaraciones de conformidad, registro de sistemas de alto riesgo, responsables autorizados de IA;

⇒ El derecho a la protección de los derechos de los menores de edad en el entorno digital;

⇒ El derecho a no recibir publicidad dirigida;

⇒ El derecho a no ser objeto de decisiones individuales automatizadas;

⇒ El derecho a estar protegidos frente a contenidos ilícitos o engañosos, o frente a cualquier acto engañoso de los proveedores que inste a proporcionar datos personales, suscribirse a servicios o contenidos o comprar productos o servicios concretos bajo engaño o aceptar publicidad comportamental;

⇒ El derecho a cambiar de plataforma o conseguir la interoperabilidad entre contenidos o servicios de distintas plataformas digitales;

⇒ El derecho a denunciar prácticas desleales o engañosas, así como a denunciar contenidos ilícitos, nocivos o prácticas que vulneren la libertad de expresión o pensamiento, la libertad de acceso a la información y la libertad de opinión;

⇒ El derecho a plantear quejas y formular reclamaciones, acudiendo a los sistemas de resolución extrajudicial de conflictos, no solo a los que están disponibles en sistemas de comercio electrónico, sino también para cualquier servicio o contenido que se ponga a disposición en el entorno digital;

⇒ El derecho a la protección de nuestros derechos como usuarios o consumidores de productos y servicios digitales

Las autoridades públicas nacionales y europeas creadas tienen la obligación de vigilar que estos derechos estén protegidos y se hagan efectivos, vigilando a los proveedores de servicios y contenidos digitales y a las empresas desarrolladoras, importadoras o suministradoras de sistemas de IA.

Conclusiones:

En este artículo hemos podido conocer distintas normativas europeas aplicables al entorno digital, las obligaciones a cumplir por parte de las empresas proveedoras de contenidos y servicios digitales, incluyendo sistemas de IA, y los perfiles jurídicos que en algunos casos, se están creando para el cumplimiento normativo: figuras ya conocidas como el **Delegado de protección de datos (DPO),** que en los últimos meses están cobrando protagonismo, si asumen funciones como responsable de IA, director de datos o responsable de los proyectos digitales de una organización, aunando funciones como **responsable autorizado de sistemas de IA**, ya que algunas funciones, como las de custodiar documentación técnica y jurídica, verificar el cumplimiento legal o ser el punto de contacto con las autoridades, parece que coincide con las propias de un DPO; otras figuras nuevas, como **guardianes de acceso**, que serán las propias empresas proveedoras de contenidos y servicios digitales, o los **alertadores de confianza**, en este caso, aún por implantar (pueden ser entidades de gestión colectiva de derechos de autor o conexos las que asuman ese papel).

Estos perfiles, junto a los organismos nacionales y europeos encargados del control y supervisión de las normativas, deberán trabajar para que los usuarios de los servicios y contenidos digitales, puedan estar presentes y consumir en el entorno digital, con plena garantía de sus derechos fundamentales y libertades públicas. Las normativas europeas se traducen en obligaciones, aunque por el momento se aplican en mayor medida a grandes compañías digitales; sí que tiene una implantación total la normativa de protección de datos personales, también en el desarrollo y uso de sistemas de IA que supongan un tratamiento de información de los usuarios. El Delegado de protección de datos, el responsable de IA, o un perfil que realice funciones conjuntas, como responsable de datos o de proyectos digitales, será lo más próximo que veamos en el futuro empresarial.

Nota final:

Me preguntan constantemente por las obligaciones legales que imponen las últimas normativas europeas aplicables al entorno digital. Espero haber arrojado un poco de luz al respecto. Mi conclusión es que la figura del Delegado de protección de datos o DPO, figura ya habitual en muchas empresas y entidades jurídicas, seguirá asumiendo nuevas funciones, también en el desarrollo, distribución, importación, implantación o uso de sistemas de IA, ya que estos sistemas pueden suponer el tratamiento de datos personales. Lo estoy comprobando cada día: pymes y organizaciones que utilizan imágenes, o audios con la voz de personas reales, para generar contenidos digitales, utilizando IA; esas personas reales pueden ser sus propios empleados, sus propios clientes o usuarios de sus plataformas digitales. Será imprescindible aplicar la normativa de protección de datos, realizar una previa evaluación de impacto del uso de estos sistemas de IA, inventariar las herramientas de IA utilizadas en los registros de actividades de tratamiento, así como revisar estos tratamientos, cómo funcionan los modelos de IA en cuanto a la entrada y salida de datos, o si se usan para la toma de decisiones automatizadas, analizando a su vez las bases que legitiman el tratamiento (consentimiento, interés legítimo, ejercicio de funciones públicas), y adaptando todos los instrumentos jurídicos que informan y recogen estos consentimientos. Por supuesto, el DPO además realizará en muchos entornos empresariales o públicos estas funciones nuevas en relación a sistemas de IA, sin olvidar que debe ejercer estas funciones con plena independencia y evitando cualquier conflicto de interés (una misma persona no puede implementar actividades de tratamiento de datos y a la vez revisar y vigilar el cumplimiento de la LOPD).

En cuanto a las funciones supervisoras de autoridades y organismos públicos ya conocidos y también de las nuevas autoridades públicas que se están creando, veremos si sus funciones no quedan limitadas a la tan temida capacidad sancionadora. Esperemos que trabajen todas ellas en beneficio de los derechos de los usuarios.

Conchi Cagide Torres.

Bibliografía y otras referencias

Artículo "the data act & policy options for a sectoral regulation to protect competition in the automotive aftermarket", JIPITEC 2/2024 (vol. 15)- [Fecha consulta: 10 Septiembre 2024].

Informe "Is the DPO the right person to be the AI officer", julio 2024, de la CEDPO– Confederation or Europea Data Protection Organisation.

Sentencias del Tribunal de Justicia Europeo analizadas:
STJUE C-453/21, asunto X-FAB
STJUE C-534/20, asunto Leishitz
STJUE C-634/21, asunto SCHUFA

Webs:
https://digital-markets-act-cases.ec.europa.eu/search (web de la Comisión Europea donde se pone a disposición los documentos de designación de guardianes de acceso)
https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (web de la Comisión Europea donde se informa de las plataformas digitales y servicios obligados al cumplimiento de la DSA).
https://digital-strategy.ec.europa.eu/es/policies/trusted-flaggers-under-dsa (listado de alertadores de confianza publicado por la Comisión Europea) [fecha consulta 13 diciembre 2024]

Puedes acceder a todos los artículos de investigación en la web www.intangia.com

Autora: Conchi Cagide Torres. Directora del Departamento jurídico de Intangia

Para citar a la autora:

 ISNI: 0000000506286844