ENE'23

RSM DIGITAL #9

Multa a Facebook por no evitar técnicas de Data Scraping

El pasado 25 de noviembre de 2022, la Data Protection Comission (en adelante, "DPCI"), autoridad de control en materia de privacidad y protección de datos de Irlanda, emitió un comunicado mediante el cual anunciaba que, tras la conclusión de un procedimiento sancionador iniciado en abril de 2021, Facebook sería sancionada con una multa de 265 millones de euros y la adopción de una serie de medidas correctoras por no evitar el *"data scraping"* de sus usuarios.

¿Qué es el data scraping?

El *data scraping* o "raspado" de datos es una técnica que permite a quien la utiliza obtener datos a partir de la lectura de un sitio web mediante la utilización de un software automatizado, tras lo cual se puede distribuir dicha información en foros online o ser utilizada para fines propios.

El objetivo básico de la extracción u obtención de los referidos datos es el de estudiar patrones de comportamiento y tendencias recurrentes con el fin de predecir las necesidades o gustos de los usuarios propietarios de los datos extraídos.

Es decir, la obtención de este tipo de datos o información permite a las empresas impulsar sus decisiones comerciales y ofrecer al usuario ciertos productos o servicios en función de sus preferencias concretas.

Investigación llevada a cabo por la Comisión de Protección de Datos de Irlanda

Durante la investigación efectuada a la gigante americana por la DPCI, se pudo comprobar que los datos de más de 530 millones de usuarios de Facebook se encontraban expuestos en internet, datos tales como las direcciones de correo electrónicos de los afectados o sus números de teléfonos móviles, por un fallo en los sistemas de seguridad de la propia Facebook.

En este sentido, y durante el período comprendido entre el 25 de mayo de 2018 y el mes de septiembre de 2019, la DPCI efectuó una exhaustiva evaluación sobre las herramientas: *"Facebook Search"*, *"Facebook Messenger Contact Importer"* e *"Instagram Contact Importer"*, en relación con el tratamiento de datos realizado por parte de Meta Platforms Ireland Limited, concluyendo dicha evaluación en que la empresa habría infringido el artículo 25 del Reglamento General de Protección de Datos (RGPD) debido a la falta de implementación de medidas técnicas y organizativas adecuadas para evitar el mencionado *"data scraping"*.

Teniendo en cuenta lo anterior, la DPCI determinó que, debido al gran volumen de datos afectados, el hecho de que en la empresa ya existían precedentes de scraping y que Facebook podría haber identificado con suficiente antelación que esta técnica estaba siendo utilizada sobre los datos de sus usuarios, procedía la imposición de una multa significativa por exponer a los afectados a un riesgo considerable, cuya consecuencia era la pérdida del control sobre sus datos siendo expuestos a estafas, spam y phishing.

Precisamente por este motivo, y en aras a evitar la utilización de técnicas de scraping como la que nos atiene y posibles sanciones, varias empresas de blockchain han optado por desarrollar aplicaciones de redes sociales de blockchain que no requieren que los usuarios faciliten determinados datos como, por ejemplo, sus direcciones de correo electrónico o números de teléfonos. De hecho, los desarrolladores de Ethereum (tecnología que alberga dinero digital, pagos globales y aplicaciones) han creado un sistema de autenticación llamado "EIP-4361" que aún se encuentra en fase de prueba pero cuyo objetivo será estandarizar el proceso de inicio de sesión de la billetera en todas las aplicaciones, eliminado la necesidad de solicitar a sus usuarios información personal y previniendo violaciones como la ocurrida en Facebook.

José María Baños
Partner | Lawyer

Área de Negocio Digital de RSM Spain
E jbanos@rsm.es

N° 8 | ENERO DE 2023

Carmen Araolaza

Área de Negocio Digital de RSM Spain
E caraolaza@rsm.es

Cómo hacer que tu evaluación de impacto tenga éxito

El RGPD introdujo el concepto de Evaluación de Impacto relativa a la Protección de Datos (EIPD). A partir de ese momento, **es obligatorio para las Autoridades de Control establecer listas orientativas de tratamientos que no requieren evaluaciones de impacto**, así como de tratamientos que sí requieren su realización.

¿Qué es una evaluación de impacto y para qué sirve?

La EIPD es una herramienta que faculta a quien la utiliza a evaluar de manera anticipada cuáles son los **potenciales riesgos a los que se exponen los datos personales** en función de las actividades de tratamiento que se estén llevando a cabo en ese proyecto en concreto. Se busca posibilitar que los responsables del tratamiento adopten las medidas que reduzcan los riesgos producidos, **disminuyendo la posibilidad de su materialización** y las consecuencias negativas de los interesados.

Sirve, en definitiva, como un ejercicio para analizar los riesgos que un determinado sistema de información, producto o servicio puede traer consigo en lo relativo a la protección de los datos personales de los interesados. Se busca conseguir la **correcta gestión de dichos riesgos a través de la adopción de las medidas necesarias para eliminar o atenuar en gran parte** o en la mayoría de lo posible aquellos riesgos que hayan sido identificados.

Pasos y requisitos para hacer una evaluación de impacto exitosa

Los requisitos para la realización de una evaluación de impacto exitosa es que se realice cuando lo exija el RGPD, esto es, cuando el tratamiento pueda entrañar un **alto riesgo para los derechos y libertades de las personas**.

En este sentido, resulta importante señalar que la realización de una EIPD **no es obligatoria en todos los casos**, aunque sí que resulta recomendable en muchas situaciones donde se realice un tratamiento de datos. Solamente es obligatorio cuando este tratamiento pueda entrañar un riesgo alto para los derechos y libertades de los usuarios.

En concreto, será obligatoria cuando suponga la evaluación sistemática y exhaustiva de aspectos personales de una persona, incluida la elaboración de perfiles, cuando se realice un tratamiento a gran escala de datos sensibles, y cuando se realice una observación sistemática a gran escala de una zona pública.

Cómo implementar una evaluación de impacto paso a paso

Para la realización de una EIPD se distinguen varias fases:

1. **Necesidad de una EIPD**
   En esta fase se realiza una valoración de la conveniencia de llevar a cabo o no una Evaluación de Impacto.

2. **Descripción del proyecto y los flujos de información**
   En esta fase se realiza un análisis en profundidad del proyecto, donde habrá que analizar, entre otros, las categorías de datos que se tratan, los usuarios de los mismos, los flujos de información y tecnologías utilizadas.

3. **Identificación y evaluación de riesgos**
   Se analizarán los posibles riesgos para la protección de datos de los afectados y se valorará la probabilidad y el impacto de su materialización.

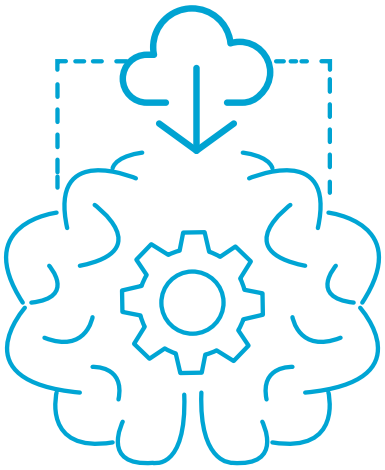
Carmen Araolaza

Área de Negocio Digital de RSM Spain
E caraolaza@rsm.es

4. **Medidas para garantizar la privacidad de los datos personales**
   Esta fase supone la identificación de las medidas necesarias para eliminar, mitigar, trasladar o asumir los riesgos detectados.

5. **Informe final**
   El informe final será aquella fase donde se realizará un análisis detallado de los riesgos que hayan sido identificados, así como de las recomendaciones y propuestas para eliminarlos o mitigarlos.

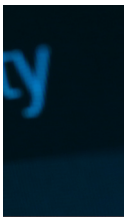
6. **Revisión**
   Esta última fase sirve para verificar la efectividad de la EIPD y examinar si se han creado nuevos riesgos o se han detectado otros que se habían detectado con anterioridad.



En RSM somos expertos en protección de datos, y podemos asesorarte tanto en tu evaluación de impacto y ayudarte en todas las fases de su desarrollo. ■

Marc Gallardo
Partner | Lawyer

Área de Negocio Digital de RSM Spain
E mgallardo@rsm.es



¿De qué Startups hablamos cuando hablamos de la Ley de Startups?

La Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes, más conocida como **Ley de Startups**, entró en vigor el 23 de diciembre con el propósito de impulsar la creación y crecimiento de este tipo de empresas, estableciendo para ello un conjunto de beneficios y especialidades de carácter fiscal, laboral, societario y administrativo.

Ahora bien, ***¿qué empresas se consideran emergentes a los efectos de esta Ley y por tanto susceptibles de beneficiar de sus medidas?***

Se entiende por **empresa emergente** a toda persona jurídica (sociedades de capital y cooperativas) que reúna simultáneamente las siguientes condiciones:

1) Ser de nueva creación o, no siéndolo, cuando no hayan transcurrido más de 5 años desde la inscripción de su constitución en el Registro Mercantil o Registro de Cooperativas competente, o de 7 años en el caso de empresas de biotecnología, energía, industriales y otros sectores estratégicos que se determinarán por orden ministerial.

2) No haber surgido de una operación de fusión, escisión, segregación, concentración o transformación de empresas que no tengan consideración de empresas emergentes.

3) No distribuir ni haber distribuido dividendos o retornos en el caso de cooperativas).

4) No cotizar en un mercado regulado.

5) Tener su sede social, domicilio social o establecimiento permanente en España.

6) Tener al 60% de la plantilla con un contrato laboral en España.

7) Desarrollar un proyecto de emprendimiento innovador que cuente con un modelo de negocio escalable. Se considera que una empresa emergente es innovadora cuando su finalidad sea resolver un problema o mejorar la situación existente mediante el desarrollo de productos, servicios o procesos nuevos o mejorados sustancialmente en comparación con el estado de la técnica y que lleve implícito un riesgo de fracaso tecnológico, industrial o en el propio modelo de negocio. La Ley prevé unos criterios mínimos para evaluar el requisito del emprendimiento innovador y de la escalabilidad del modelo de negocio de la empresa emergente.

Si la empresa emergente pertenece a un grupo de empresas (definido en el artículo 42 del Código de Comercio), el grupo o cada una de las empresas que lo componen deberá cumplir con los requisitos anteriores.

¿Qué empresas quedan automáticamente excluidas de la Ley Startups?

No podrán acogerse a los beneficios de esta Ley aquellas empresas emergentes fundadas o dirigidas por sí o por persona interpuesta que no estén al corriente de las obligaciones tributarias y con la Seguridad Social, hayan sido condenadas por sentencia firma por la comisión de alguno de los tipos delitos mencionados en la Ley o hayan perdido la posibilidad de contratar con la Administración.

¿Quién valida el cumplimiento de los anteriores requisitos?

La Empresa Nacional de Innovación SME S.A. **(ENISA)**.

La validación deberá hacerse con carácter previo a la inscripción de la condición de empresa emergente en el Registro Mercantil o de Cooperativas competente.

El procedimiento de evaluación por parte de ENISA se efectuará en un plazo no superior a 3 meses a contar desde la fecha en que la solicitud y documentación completa con toda la información requerida haya tenido entrada en el registro electrónico que se habilita a tal fin.

El vencimiento de dicho plazo sin que se haya notificado resolución expresa legitima al solicitante para entenderla estimada por **silencio administrativo positivo**.

¿Por qué es necesaria la inscripción de la condición de empresa emergente en el Registro Mercantil?

La inscripción de la condición de empresa emergente inscrita en el Registro Mercantil o en el Registro de Cooperativas será condición necesaria y suficiente para poder acogerse a los beneficios y especialidades de esta Ley.

El Registro Mercantil habilitará un procedimiento de consulta en línea gratuito para cualquier persona interesada en conocer la condición de empresa emergente de una determinada sociedad. ■

Marta Moreno

Área de Negocio Digital de RSM Spain
E caraolaza@rsm.es

Brechas de datos personales: Cómo actuar

El desarrollo de las nuevas tecnologías nos ha convertido en testigos del incremento de los riesgos para el derecho al respeto de la vida privada, desencadenando en la necesidad de contar con normas que regulen específicamente el tratamiento de información personal de los ciudadanos.

Paralelamente, sufrir un incidente de seguridad se ha convertido en una cuestión de probabilidades. Ésta es una realidad difícil de asumir, no sólo desde el punto de vista técnico, sino también por las consecuencias económicas que puede ocasionar en la empresa.

Por tanto, corresponde intentar evitar las brechas de datos personales y, en caso de que sucedan, **gestionarlas adecuadamente**, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

¿Qué es una brecha de datos personales?

Si bien todas las brechas de datos personales son incidentes de seguridad de la información, no todo incidente de seguridad es necesariamente una brecha de datos personales.

La Agencia Española de Protección de Datos (en adelante, "AEPD") define una brecha de seguridad como "un incidente de seguridad que ocasione la **destrucción, pérdida o alteración accidental o ilícita de los datos personales** tratados por un responsable, o bien la **comunicación o acceso no autorizados a los mismos**".

Por tanto, para que un incidente sea calificado como brecha de datos personales se requiere una **afectación de datos personales**.

¿Cuándo debe notificarse una brecha de seguridad a los interesados?

De conformidad con el artículo 34 del Reglamento General de Protección de Datos (en adelante, RGPD), los responsables de un tratamiento de datos tienen la **obligación de comunicar a las personas afectadas** aquellas brechas de datos personales que puedan entrañar un riesgo alto para sus derechos y libertades.

Si bien la guía elaborada por la AEPD en 2018 establecía una sencilla fórmula matemática para discernir la necesidad (o no) de comunicar la brecha, la nueva guía obvia todo criterio matemático para centrarse en la importancia de analizar la naturaleza y las consecuencias de cada brecha de forma individualizada.

En concreto, se establecen como requisitos fundamentales a estos efectos: (i) **analizar la severidad del riesgo generado por la brecha, (ii) la probabilidad de que este riesgo se materialice y (iii) la afectación a Derechos Fundamentales**.

Protocolo a seguir ante una brecha de seguridad de datos personales en tu empresa

Ante una brecha de datos personales, corresponde elaborar un plan de acción organizado en el que, entre otras, se especifiquen acciones destinadas a determinar la raíz de ésta; concretar la extensión, el impacto y la severidad de sus efectos; o neutralizar sus daños.

Asimismo, de conformidad con el RGPD, las empresas deberán **documentar cualquier violación de la seguridad** de los datos personales, incluyendo detalles de los hechos, sus efectos y las medidas correctivas adoptadas. Esta obligación se torna esencial en el contexto de ser investigados por la AEPD, ya que la documentación elaborada permitirá a la autoridad de control verificar el cumplimiento con las obligaciones impuestas en el RGPD.

Cabe señalar que, además de la obligación de notificar la brecha a los interesados, el RGPD en su artículo 33 impone a los responsables de un tratamiento de datos personales la obligación de **notificar a la autoridad de control competente** las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

En conclusión, una brecha de datos personales puede ser la semilla de la que germinen **efectos adversos de importante magnitud** para las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Por ello, desde Letslaw by RSM recomendamos tomar conciencia e implementar medidas de prevención –que llevan implícitos costes económicos– aunque a priori no se traduzcan en un retorno de la inversión claro, ya que a la larga reducirán el riesgo de sufrir este tipo de brechas.

En todo caso, el resgo cero no existe y ante una brecha de seguridad, lo más recomendable es ponerse en manos de expertos en la materia que puedan analizar la casuística de conformidad con la legislación vigente para así evitar infracciones que pueden resultar en costosas multas.

RSM cuenta con especialistas en materia de derecho digital dispuestos a ayudarte para prevenir una brecha de seguridad o paliar los efectos de ésta si ya se hubiera producido. ■

Vincenzo Lo Coco

Área de Negocio Digital de RSM Spain
E vcoco@rsm.es

Gestionar mal las cookies de la página web puede costar caro: todo lo que tenemos que aprender de las multas millonarias a los gigantes tecnológicos

A principio del nuevo año, la *Commission Nationale de l'Informatique et des Libertés* (CNIL), la autoridad de control en materia de protección de datos en Francia, ha impuesto una multa de 5 millones de euros al proveedor de la red social TikTok por no haber implementado en su página web mecanismos sencillos e inmediatos para que los usuarios pudieran revocar el consentimiento para las cookies y por no haber establecido, de manera suficientemente precisa, los fines para los que estas se recogen.

La sanción, si bien referida a una de las redes sociales más populares del momento, debe poner en alerta a todas las empresas también en España.

En la actualidad, la mayoría de las páginas web y apps de empresas españolas no cumple con las normas sobre las cookies – esto es el art. 22 de la Ley de la Sociedad de la Información (LSSI).

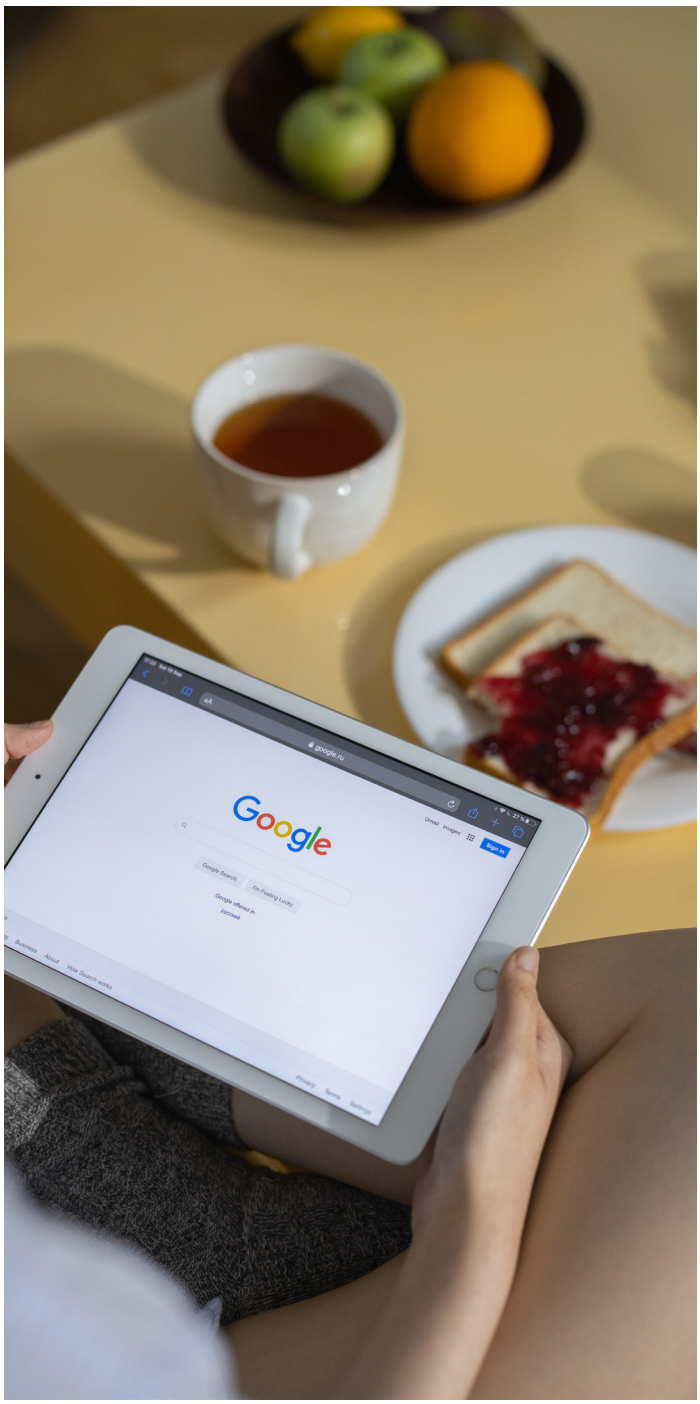
¿Cómo pueden evitarse las sanciones por incumplimiento?
Teniendo en cuenta las recomendaciones de la Agencia Española de Protección de Datos (AEPD) recogidas en la *Guía sobre el uso de las Cookies* (la versión más actualizada es la publicada en Junio de 2022), para no correr el riesgo de verse imponer una sanción es necesario revisar (o identificar) las cookies que se están utilizando, analizar si son cookies propias o de terceros, de sesión o persistentes, y averiguar cuál es su función.

A partir de esta revisión, será necesario asegurarse de informar adecuadamente a los usuarios sobre la utilización de las cookies y, en particular, sobre sus fines, de acuerdo con lo dispuesto en el art. 22 de la LSSI. La información debe ser suficientemente completa para permitir a los usuarios entender sus finalidades y el uso que se les dará.

Finalmente, la página web debe contar con mecanismos para recabar el consentimiento de los usuarios que sean conformes a la normativa vigente. Al respecto, es importante tener en cuenta que de permanecer visualizando la pantalla, hacer *scroll* o seguir navegando por el sitio web no se considerará una clara acción afirmativa y puede exponer al responsable de la página web a sanciones.

Será necesario que el usuario realice una acción que pueda calificarse como una clara acción afirmativa para que el consentimiento al uso de las cookies se considere válidamente otorgado. Asimismo, retirar el consentimiento debe ser tan fácil como prestarlo.

Los avisos de cookies que se implementen en las páginas web deberán tener en cuenta estos principios básicos para no exponer la empresa responsable de la página web al riesgo de sanciones.



RSM Spain
BARCELONA | MADRID | GRAN CANARIAS | PALMA DE MALLORCA | TARRAGONA | VALENCIA

rsm.es

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM