Expediente N.º: EXP202306252
IMI Reference: Case Register 570191

RESOLUCIÓN DE PROCEDIMIENTO DE APERCIBIMIENTO

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes Antecedentes, Hechos Probados y Fundamentos de Derecho, la Directora de la Agencia Española de Protección de Datos resuelve adoptar la presente resolución de apercibimiento.

TABLA DE CONTENIDO

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante), representado por NOYB (European Centre for Digital Rights, Goldschlagstraße 172/4/3/2, 1140 Vienna, ZVR: 1354838270), con fecha 21 de agosto de 2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra FREEPIK COMPANY S.L. con NIF B93183366 (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

- A través de código HTML incrustado en la página **web ****URL.1***, el 14 de agosto de 2020 se han recogido datos personales de la parte reclamante y se han transferido a EEUU a través de los servicios de Facebook (incluyendo Facebook Connect) contratados por el responsable del portal, FREEPIK COMPANY S.L.

- La parte reclamante manifiesta que, durante la visita por su parte al mencionado sitio web, la cual tuvo lugar mientras se conectaba a la cuenta de Facebook asociada a su dirección de correo electrónico, la parte reclamada trató sus datos personales (al menos, la dirección IP y "cookies"), y, que algunos de estos datos han sido transferidos a Facebook Inc. en los EEUU.

- La parte reclamante sostiene que la transferencia de datos personales a EEUU por parte de la parte reclamada, bien a través de Facebook Ireland como intermediario o directamente a Facebook Inc., carecía de base jurídica, toda vez que el TJUE había invalidado la decisión sobre el "EU-US Privacy Shield" en el fallo C-311/18 ("Schrems II"), y la parte reclamada ya no podía basar la transferencia de datos a Facebook Inc. en los EEUU en una decisión de adecuación en virtud del Artículo 45 del RGPD.

- La parte reclamada tampoco podía basar la transferencia de datos en las cláusulas contractuales tipo previstas en Artículo 46.2.c y 46.2.d del RGPD, si el tercer país de destino no garantizaba una protección adecuada de los datos personales transferidos con arreglo a esas cláusulas, con arreglo a la legislación de la UE. El TJUE había fallado explícitamente que las transferencias ulteriores a empresas comprendidas en el artículo 50 del Código de los Estados Unidos (USC), como es el caso de Facebook, violaban los artículos pertinentes del Capítulo 5 del RGPD, ya que, en virtud de esta normativa (50 USC § 1881ª, o "FISA 702"), estaban sujetas a la vigilancia de la inteligencia de EEUU. Como se desprende de las "Snowden Slides" y del propio Transparency Report de Facebook, esta entidad estaba proporcionando activamente datos personales al gobierno de los EEUU bajo ese precepto.

- La parte reclamada y Facebook habían seguido confiando en el "EU-US Privacy Shield" y en las cláusulas estándares de protección de datos para las mencionadas transferencias de datos.

Junto a la reclamación se aporta:

01 – Condiciones de Facebook de las herramientas empresariales
02 – Condiciones de Facebook del tratamiento de los datos
03 – Nuevas Condiciones de Facebook las herramientas empresariales
04 – Nuevas Condiciones de Facebook del tratamiento de los datos

05 – Datos HAR de la visita al Sitio Web con, entre otro, el siguiente contenido: tres peticiones GET y una petición POST
06 – Condiciones del Escudo de la privacidad
07 - Facebook Inc. y El Escudo de la Privacidad de la UE y los EEUU y de Suiza y los EEUU
08 - “Snowden Slides”
09 – Acuerdo de representación

SEGUNDO: A través del “Sistema de Información del Mercado Interior” (en lo sucesivo Sistema IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, esta Agencia comunicó esta reclamación, de conformidad con lo establecido en el artículo 56 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, 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 (en lo sucesivo, RGPD), teniendo en cuenta su carácter transfronterizo y que esta Agencia es competente para actuar como autoridad de control principal, dado que la parte reclamada tiene su establecimiento en España.

Los tratamientos de datos que se llevan a cabo afectan a interesados en varios Estados miembros. En el presente caso, de conformidad con lo establecido en el artículo 60 del RGPD, actuarían en calidad de “autoridad de control interesada”, las autoridades de todos los Estados Miembro, todas ellas en virtud del artículo 4.22 del RGPD, dado que los interesados que residen en el territorio de estas autoridades de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

TERCERO: Con fecha 5 de octubre de 2020, de conformidad con el artículo 64 de la entonces vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

1) Mediante diligencia realizada por esta Agencia en fecha 25 de octubre de 2023, se comprobó que en el plenario del Comité Europeo de Protección de datos de fecha 2 de septiembre de 2020, se decidió crear un grupo de trabajo (en adelante, “TF101”) para asegurar una aproximación coherente entre las autoridades de datos europeas para gestionar las 101 reclamaciones de NOYB, que versaban sobre cuestiones similares (quien reclamaba había visitado una página web de un responsable de tratamiento mientras había iniciado sesión en su cuenta de Google o Facebook, vinculada a su dirección de correo electrónico. Y el responsable de tratamiento había embebido

código de servicios de Google o Facebook, que habían transferido sus datos personales a Estados Unidos, sin tener base jurídica para ello).

2) En respuesta al requerimiento de información efectuado por esta Agencia, con fecha 11 de diciembre de 2020 la parte reclamada remitió a esta Agencia la siguiente información y manifestaciones:

1. Que "Facebook Connect" era la herramienta que, en su momento, permitía el registro de usuarios utilizando credenciales de FACEBOOK en lugar de crear un nombre de usuario y contraseña específicos para el servicio. Que en la actualidad se denominaba "Facebook Login".

2. Que las webs de la parte reclamada tenían en ese momento incrustado el código de "Facebook Login".

3. Que utilizaban "Facebook Login" como identidad federada. Que de esta manera se trataban de forma separada los datos de usuario y por otro lado la contraseña, lo que evitaba que, en caso de sufrir una brecha de seguridad, la contraseña del usuario pudiera ser accedida por el atacante. Que, además, se mejoraba la experiencia del usuario ya que le permitía completar el procedimiento de registro de forma más ágil.

4. Que el funcionamiento de "Facebook Login" era el siguiente:
"[…]
En el caso del "inicio de sesión o login de Facebook" cuando el usuario decide crear su cuenta usando sus credenciales de FACEBOOK, y pulsa el botón de la red social, se produce una llamada a la API de FACEBOOK, que abre una ventana en la que el usuario tiene que introducir su correo electrónico y contraseña de su cuenta de FACEBOOK para que se pueda completar el proceso de registro.
En dicha ventana, controlada por FACEBOOK -no por FREEPIK, el usuario es informado de que FACEBOOK compartirá con FREEPIK ciertos datos para llevar a cabo el proceso de registro, tales como nombre, fotografía y dirección de correo electrónico. Sólo cuando el interesado ha prestado su consentimiento específico a este tratamiento, el proceso termina y la cuenta de usuario es creada en FREEPIK. FREEPIK recibe solamente el nombre de usuarios, cuenta de correo electrónico y fotografía del usuario).
[…]"

5. Que respecto a "Facebook Login", dependiendo de la configuración, permitía obtener, previa aprobación por el interesado, de una cantidad de datos personales de distinto alcance, como p.ej. el listado de amigos en FACEBOOK, las páginas a las que se ha dado a "like", la localización o el género. En el caso de la parte reclamada, solo solicitaban y obtenían, previo consentimiento, los datos mínimos posibles: nombre de usuario, dirección de email y fotografía.

Se aporta captura de pantalla donde consta como campo obligatorio el nombre y la foto de perfil y como campo opcional, la dirección de correo electrónico. Consta asimismo el siguiente texto "*Política de privacidad y Condiciones de Freepik Company*" donde las palabras "*Política de privacidad"* y "*Condiciones"* son hiperenlaces.

6. Respecto al funcionamiento de “Facebook Pixel”, su configuración y al consentimiento asociado manifestó:

“[…]

Además de lo anterior, el usuario puede aceptar o rechazar la instalación de cookies y tecnologías análogas como pixeles. Este proceso se realiza siempre con el consentimiento granular del usuario, gestionado a través del CMP de One Trust que FREEPIK utiliza. El usuario obtiene la información relevante en primera y segunda capa en el propio CMP y en la Política de Cookies de FREEPIK, que consideramos muy completa.

Pese a que entendemos que no es objeto de la denuncia, el píxel de marketing de FACEBOOK, se descarga en el equipo del usuario a través del CMP de One Trust que FREEPIK utiliza. El usuario, al acceder a la web, obtiene la información relevante sobre los tratamientos realizados a través de cookies y tecnologías análogas en primera y segunda capa en el propio CMP y en la Política de Cookies de FREEPIK, que consideramos muy completa.

A través del CMP el interesado puede aceptar o rechazar en bloque o granularmente las distintas finalidades ofrecidas (con las cookies aparejadas a las mismas). Es en el momento en que el usuario presta su consentimiento y éste es almacenado por One Trust cuando el píxel de FACEBOOK se instala en su dispositivo y, por tanto, comienza a recolectar información sobre dicho usuario y remitirla directamente a FACEBOOK.

Sin perjuicio de lo anterior, el usuario puede igualmente bloquear desde su propio navegador la instalación de este tipo de cookies y herramientas de seguimiento, (a través de las opciones de configuración del navegador, o añadiéndole plugins dedicados al afecto).

[…]”

También manifestó:

“El píxel de FACEBOOK es un código que funciona como herramienta de análisis y nos permite medir la eficacia de las campañas de publicidad al conocer las acciones que los usuarios realizan en nuestra web.

Una vez instalado en la web, permite recoger información sobre ciertas interacciones de los visitantes en la web, a través de la configuración de ciertos "eventos". Un evento es un tipo concreto de acción que realiza un usuario, que queda registrada a través del píxel, por ejemplo, la acción de comenzar el proceso de contratación de una suscripción premium en nuestra web.

Una vez la herramienta detecta que la actividad de un visitante activa uno de los eventos, se registra la información de dicho visitante y se envía a FACEBOOK.

A la hora de configurar la herramienta, FACEBOOK permite dos tipos de configuración: una más sencilla, que consiste en seleccionar eventos entre aquellos ya predeterminados por FACEBOOK, y otra más compleja, que permite a las empresas crear un evento propio que registrar, lo que requiere de habilidades de desarrollo informático.

Los eventos estándar que ofrece de forma predeterminada FACEBOOK son los siguiente 18 ******URL.2****)*

[…]

De los eventos descritos anteriormente, FREEPIK únicamente ha seleccionado aquellos imprescindibles para poder realizar una valoración eficaz de nuestras campañas. En concreto, actualmente tenemos activos los siguientes:

1. Página Vista: este evento es el único que viene incluido como parte del código base del píxel. Este evento indica cuándo llega alguien al sitio web con el código base del píxel instalado. El resto de eventos estándar se activan
2. Contenido Visto
3. Añadir al Carrito (actualmente no se usa)
4. Registro
5. Compra (Suscripción)

En ningún momento obtenemos información alguna de los usuarios a los que FACEBOOK impacta con publicidad. La única información que recibimos es agregada y estadística, para poder hacer seguimiento del rendimiento de las campañas y confirmar la facturación por parte de FACEBOOK."

Y aclaraba que:

a. Se permitía utilizar 18 eventos pero la parte reclamada solo utilizaba 5 y no había creado eventos personalizados.
Se aporta captura de pantalla donde constan solo los 5 eventos.

b. Que FIL (Facebook Irlanda) y sus encargados del tratamiento eran los que accedían a datos mediante la herramienta, los cuales eran anonimizados mediante agregación antes de suministrar a la parte reclamada el resultado estadístico de cada campaña.

Respecto a las audiencias personalizadas manifestó:

"A partir de la información que FACEBOOK aporta como resultado del funcionamiento del píxel (información agregada, en ningún caso obtenemos información individualizada de los visitantes de la web cuya actividad ha sido registrada a través del píxel), se crean las "Audiencias Personalizadas", es decir; "grupos" de usuarios de FACEBOOK a los que se mostrarán anuncios de FREEPIK en función de sus acciones y comportamientos en nuestra web.
Estas audiencias pueden ser creadas a partir de una franja de edad concreta o una localización geográfica específica, que el cliente de FACEBOOK selecciona. FACEBOOK no comparte información sobre aquellos usuarios a los que se ha impactado con publicidad, únicamente se ofrece información agregada.
FACEBOOK permite crear hasta 500 audiencias personalizadas por cuenta publicitaria. En FREEPIK no llegamos a 80 Audiencias Personalizadas, algunas ya no se usan y muchas son duplicadas por mercado (EN .com), (ES .es), etc..."

Respecto a las audiencias similares manifestó:

"Las audiencias similares son una forma de llegar a aquellas personas nuevas que tienen más probabilidades de interesarse por nuestra empresa, ya que se parecen a nuestros clientes actuales. Es decir; vamos a mostrar nuestra publicidad a personas parecidas (o similares) a las que ya interactúan con nuestra empresa. Igualmente, no obtenemos información sobre estos usuarios de FACEBOOK que se consideran "similares" a aquellos que han visitado nuestra web. Únicamente obtenemos información de forma agregada y estadística.
FACEBOOK ofrece otras alternativas de configuración en relación con la información que puede recabar el píxel, para que éste pueda de forma

automática y sin necesidad de configurar el código, buscar información relevante a lo largo de la web.
Con el objetivo de tener un control más transparente de la información compartida con FACEBOOK, no tenemos activada la siguiente opción."
Y aporta una captura de pantalla donde consta que la opción de *"Hacer un seguimiento de los eventos automáticamente sin código*" está desactivado.

7. Que respecto al plazo de conservación de los datos recogidos, en ******URL.3*** constaba *"[…]Con arreglo a las presentes condiciones podemos conservar los Datos de eventos durante un periodo máximo de dos años. Conservaremos cualquier audiencia que hayas creado usando estos datos hasta que los elimines por medio de las herramientas de tu cuenta […]."*

8. Manifestó respecto a en qué países se tratan los datos personales:
"[…]
En lo que respecta a FACEBOOK IRELAND, recordar aquí que esta empresa no ha atendido nuestra solicitud de información sobre su cadena de subcontratación (alegando razones "comerciales y de seguridad"), así que más allá del obvio y manifiesto tratamiento por parte de FACEBOOK Inc, de nacionalidad estadounidense, no estamos al corriente de la identidad ni nacionalidad de ninguno de sus posibles encargados y/o subencargados de tratamiento.
[…]"

9. Que respecto a la base legal del tratamiento, incluyendo la comunicación de datos a FACEBOOK, manifestó:
"[…]
En los tratamientos de datos en los que FACEBOOK y FREEPIK son corresponsables, FREEPIK obtiene el consentimiento del interesado vía el CMP de One Trust (pixel de marketing) y FACEBOOK lo obtiene directamente de él, en relación con el "Inicio de sesión" tal y como se ha explicado en la respuesta a la cuestión 8a.
FREEPIK integra la Herramienta "Inicio de sesión" de FACEBOOK de modo que esta obtiene directamente el consentimiento del interesado al tratamiento de sus datos personales,[…].
Los tratamientos de datos realizados por FACEBOOK que exceden los tratamientos de datos anteriormente descritos, se regulan de acuerdo con los distintos textos que integran la Política de Privacidad de Facebook[…]"

10. Que, aunque entendían que no era objeto de la denuncia, aportaban también información sobre el pixel de FACEBOOK (Facebook Pixel).

11. Que no tuvo la opción de transferir o no datos a EEUU, que FACEBOOK no permitía a las empresas elegir la configuración respecto de la localización de los datos y las transferencias internacionales.

12. Que, desde el punto de vista de la parte reclamada, únicamente FIL (Facebook Irlanda) era receptora de la información. Que FIL comunicaba, a su vez, los datos obtenidos a FACEBOOK INC. y consideraba a éste responsable autónomo o subencargado, dependiendo del caso.

13. Que el inicio de sesión y el pixel de marketing estaban configurados para enviar información sobre el visitante directamente a FACEBOOK. Que FACEBOOK ofrecía un resumen de los datos tratados por sus productos en ******URL.4***

14. Que el contrato que regía su relación con FACEBOOK se encontraba en ***URL.3 .

En relación a las transferencias internacionales:

15. Que la transferencia internacional se basaba en el Apéndice sobre transferencia de datos de la UE ubicado en ***URL.5 . Que el modelo de cláusulas contractuales tipo utilizadas era el de la Comisión en 2010.

16. Aporta un documento de "*Justificación del uso de SCCs como instrumento suficiente*" y otro con una opinión legal encargada a DLA Piper.

En el primer documento consta, entre otras cuestiones:

"[…]
Normativa estadounidense relevante.
[…]
1.1.1. Executive Order 12333 y Presidential Policy Directive 28
Estas normas regulan y, más importante, limitan la capacidad de acción de inteligencia de las agencias del Gobierno de EEUU fuera de EEUU de dos modos principales.g
Finalidad de vigilancia y defensa nacional
En primer lugar, ambas limitan las finalidades de su vigilancia a la protección de la seguridad nacional, prevención del terrorismo y amenazas extranjeras análogas. No existe obligación de colaborar
En segundo lugar, además, la EO 12333 no prevé ningún mecanismo para obligar a las empresas estadounidenses importadoras a colaborar con el Gobierno. Es decir, con base en la EO 12333, los proveedores de FREEPIK en EEUU no tienen obligación de colaborar con las agencias de inteligencia para aportar datos personales de usuarios europeos, lo que resulta un hecho de gran relevancia.
1.1.2. Foreign Intelligence Surveillance Act (FISA)
[…]
Ámbito objetivo muy específico: "Foreign Intelligence Information"
[…]
De estas definiciones legales (y de los requisitos formales y materiales previstos en la normativa para los concretos requerimientos de información), se desprende Que las comunicaciones, contenidos, metadatos susceptibles de ser interceptados son únicamente aquellos Que se cruzan entre potencias extranjeras agentes n instalaciones contenido dehe estar relacionado materialmente con actividades ligadas a terrorismo. actos hostiles. armas de destrucción masiva. actividades clandestinas de espionaje. o de forma más genérica,

pero igualmente determinada, con la defensa nacional, o actividades de asuntos exteriores de los EEUU.

Es necesario identificar a la persona objeto de vigilancia

El requerimiento de información vía sección 702 debe incluir algún tipo de identificador o "selector", como una dirección de email, no puede ser indiscriminada.

Es necesario justificar el requerimiento en indicios concretos relacionados con la persona investigada y la información que se espera conseguir

De acuerdo con FISA, una Agencia de inteligencia estadounidense está obligada a aportar indicios objetivos y concretos, basados en hechos, para acreditar la probabilidad de que la persona objetivo tenga posesión, acceso o posibilidad de comunicar información relacionada con inteligencia extranjera a potencias extranjeras o a territorios extranjeros.

Además, las agencias de inteligencia también deben realizar una evaluación igualmente concreta y justificada en hechos sobre la naturaleza de la información que se espera obtener con el acceso requerido.

[…]

Capacidad de apelar el requerimiento de información.

[…]

Modificaciones posteriores a 2016

Es necesario reseñar que la sentencia Schrems ll alude a la versión de FISA en el momento en el que la Decisión de adecuación sobre el Privacy Shield se emitió, allá por 2016, y no se pronuncia sobre modificaciones posteriores, que son de alcance.

Una de las más relevantes es la que ha restringido para lo sucesivo la capacidad de requerir, con base en la Sección 702, información basada en palabras clave a encontrar en el contenido de las comunicaciones (lo que se aludía con requerimientos sobre "about") de modo que sólo se puede requerir información basada en identificadores ("selector") de la persona que emite o recibe la comunicación (lo que se alude como requerimientos "from" y/o "to").

1.2. Valoración.

De acuerdo con lo anterior (y con la Legal Opinion de DLA Piper adjunta) queda acreditado que la Normativa Relevante, si se revisa y estudia, resulta en realidad mucho más limitada de lo que en un primer momento cabría esperar.

En los apartados anteriores solamente hemos enumerado dichos límites: es imprescindible repasar las definiciones de los conceptos legales aludidos ("Foreign Intelligence Information", "Foreign Power", "Agent of a Foreign Power", "Electronic Surveillance", "Electronic Communication Service Providers') para tener una visión clara sobre el verdadero ámbito de aplicación de esta norma, que es restringido y se ubica en las antípodas de los datos que trata y exporta FREEPIK.

[…]

Es decir, la vigilancia no puede dirigirse de forma indiscriminada contra cualquier objetivo, información o persona ni dedicarse a cualquier finalidad.

De acuerdo con nuestra metodología, una vez establecido el ámbito objetivo de aplicación de la Normativa Relevante, es preciso valorar las circunstancias concretas de las transferencias internacionales de FREEPIK.

En primer lugar, la posibilidad efectiva (y objetiva) de que las autoridades nacionales del Estado importador puedan requerir acceso a los datos transferidos (en la medida en que estos sean objetivamente subsumibles en el ámbito de aplicación de la Normativa Relevante).

En segundo lugar, y en relación exclusivamente con esos "flujos o datos seleccionables", valorar el riesgo, atendiendo concretamente a las circunstancias concurrentes, de que dicha información pueda ser solicitada por las Agencias de Inteligencia "aportando indicios objetivos y concretos, basados en hechos", que acrediten que alguno de los usuarios de FREEPIK tenga posesión, acceso o posibilidad de comunicar información relacionada con inteligencia extranjera, y que sea precisamente esa información la que se obtenga mediante el requerimiento.

2. Datos personales objeto de transferencia

[…]

2.1.1. Datos personales suministrados

Hay que diferenciar diferentes tipos de interesados:

Usuarios gratuitos o visitantes: el usuario no necesita darse de alta o crear una cuenta para descargar un número limitado de imágenes o productos. Datos tratados: dirección IP y otros identificadores técnicos que se tratan para evitar el fraude, p. ej. descargas abusivas, por encima de las permitidas.

Usuarios registrados gratuitos: el tratamiento sólo comprende datos personales muy básicos, destacadamente la dirección de correo electrónico de contacto, nombre de usuario y fotografía.

Usuarios premium: sobre esta categoría se tratan, adicionalmente a los identificadores habituales anteriores, dirección fiscal, documento de identidad y datos financieros (medios de pago) almacenados y tratados únicamente por las pasarelas de pago y proveedores de dichos servicios, por razones de seguridad.

2.1.2. Datos observados

FREEPIK almacena y analiza el historial de interacciones de los usuarios con los productos disponibles en su plataforma: por ejemplo, el histórico de descargas, colaboradores favoritos, descargas gratuitas y premium, entre otras de la misma naturaleza.

2.1.3. Datos inferidos

FREEPIK analiza las interacciones de los usuarios en la web junto con datos como las búsquedas realizadas, webs de origen, de destino, descargas, o el histórico de interacciones de sus usuarios en forma agregada para tratar de inferir sus intereses.

FREEPIK analiza estos datos para inferir los productos que más interés despiertan, el momento temporal en que existen picos de demanda, la antelación respecto de eventos recurrentes, lo que le permite anticiparse y acomodar la oferta a la demanda.

[…]

2.3. Valoración.

En un análisis general, ni los datos personales objeto de tratamiento, ni las categorías de interesados, ni las finalidades de tratamiento incluyen elementos que puedan ser considerados sensibles o de categoría especial.
Además, nada de Io anterior se encuentra remotamente vinculado al ámbito de aplicación objetivo y subjetivo de la Normativa Relevante, tal y como se ha expuesto.
3. FREEPIK como potencial "Entidad Relevante"
Las condiciones exigidas en la Normativa Relevante en los apartados anteriores limitan en gran medida el alcance de la vigilancia (en especial, como hemos visto, el requisito —como condición previa- de que las agencias de inteligencia estén obligadas a justificar, con base en hechos, que no sólo los targets sino también la información que se pretende conseguir con el requerimiento de acceso, son subsumibles en el ámbito objetivo de dicha Normativa Relevante).
Desde este punto de vista, se pueden identificar situaciones en las que sea la propia organización exportadora la que represente un elemento de interés para las Agencias de Inteligencia, por su naturaleza, integrantes, o sobre todo, por su actividad.
En este sentido es preciso tener en cuenta, entre otros, elementos tales como:

- *Si la actividad del exportador en sí misma es estratégica (interesante, relevante desde el punto de vista de la seguridad nacional y los servicios de inteligencia estadounidenses).*
- *Si la actividad se califica como esencial para el normal desarrollo de las actividades cotidiana, social, política o económica del país (de modo que su interrupción forzada impactara en aquellas, p.ej.).*
- *Si se prestan servicios con acceso a datos a la Administración Pública —en cualquiera de sus niveles- o al sector público (lo que permitiría un acceso a datos de una "Potencia Extranjera").*
- *Si se tratan datos personales de políticos. altos cargos de la administración. figuras relevantes en el sector privado 11 otros individuos de interés (datos que proporcionarían información e incluso capacidad de presión sobre los mismos, así como sobre los estados o instituciones a los que representen).*
- *Si el exportador desarrolla tecnología con aplicaciones militares o de doble uso (puesto que la PPD-28 no limita la acción de espionaje sobre este tipo de tecnologías).*

Valoración
FREEPIK no se integra en la Administración Pública ni presta servicios para esta. Tampoco está sujeto a ninguna normativa relacionada con la imposición de medidas de protección por razón de su actividad (como actividades estratégicas para la seguridad nacional, actividades de interés general, actividades esenciales o especialmente relevantes, gestión o mantenimiento de infraestructuras críticas o estratégicas, etc.).
[…]
6 Conclusión
De acuerdo con lo anterior y tomando en consideración:

- *a) Por una parte, la Normativa Relevante, publicada y bien conocida (comentada en este documento y corroborada en la Legal Opinion de DLA Piper que se adjunta);*

b) Por otra, las concretas circunstancias de las transferencias de datos realizadas por FREEPIK (sobre todo, la escasa riqueza e importancia de los datos personales tratados, y su nula vinculación con el ámbito objetivo de la Normativa Relevante aplicable);

Entendemos que pura y simplemente, la Normativa Relevante no es aplicable a los datos personales exportados por FREEPIK.

De este modo, entendemos que los datos personales objeto de transferencia internacional a los Estados Unidos de Norteamérica están objetivamente fuera del alcance de las Agencias de Inteligencia de este país.

Y ello a la vista de los requisitos legales impuestos por FISA que, como condición previa, imponen que se justifique de forma particularizada y basada en hechos, la naturaleza de la información que se espera obtener con el acceso requerido (que debe estar vinculada al concepto de "Inteligencia Extranjera", en tanto que finalidad de la vigilancia).

Por tanto, entendemos que las transferencias internacionales de datos personales de FREEPIK a los Estados Unidos de Norteamérica vinculadas con la Herramienta objeto de requerimiento por la AEPD, no menoscababan el nivel de protección garantizado por el RGPD a sus titulares, ni durante la vigencia del Privacy Shield, ni con posterioridad a su anulación, desde que FACEBOOK impuso su modelo de transferencia con base en Cláusulas Contractuales Tipo.

[…]"

17. Y como conclusión manifestaba:

"[…]

Tras este análisis, FREEPIK considera que, atendidas las circunstancias concretas de la transferencia internacional de datos cuya información se requiere (y muy especialmente la naturaleza de los datos personales objeto de transferencia, a la luz de la controvertida normativa señalada en la sentencia Schrems II) los interesados -usuarios de la web de FREEPIK- no se verán afectados por las deficiencias apreciadas por dicha sentencia en la normativa de los Estados Unidos de Norteamérica.

En consecuencia, las cláusulas contractuales tipo que rigen la relación entre FREEPIK y FACEBOOK IRELAND se consideran suficientes sin necesidad de implementar medidas adicionales.

[…]

De acuerdo con todo lo anterior, consideramos que materialmente, las transferencias internacionales de datos personales que FREEPIK realiza a través de la Herramienta a FACEBOOK no menoscaban la protección reconocida por el RGPD a sus titulares.

[…]

Y nuestra interpretación era y sigue siendo, que en el caso de las transferencias realizadas por FREEPIK a través de la Herramienta, la normativa estadounidense aplicable no menoscaba el nivel de protección reconocido al interesado por el RGPD.

Nuestra evaluación de transferencias internacionales está "en proceso", y como no puede ser de otro modo, nos ponemos a disposición de la Agencia para aclarar o ampliar cualquier aspecto relacionado con este u otro requerimiento."

No se aportan garantías complementarias.

18. Manifestó también:
"[…]
En lo que respecta a FACEBOOK IRELAND, recordar aquí que esta empresa no ha atendido nuestra solicitud de información sobre su cadena de subcontratación (alegando razones "comerciales y de seguridad"), así que más allá del obvio y manifiesto tratamiento por parte de FACEBOOK Inc, de nacionalidad estadounidense, no estamos al corriente de la identidad ni nacionalidad de ninguno de sus posibles encargados y/o subencargados de tratamiento."

3) Según consta en diligencia de 28 de enero de 2021, con fecha 22 de enero 2021 se comprobó que estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, dicha visita constaba en la sección "Actividad fuera de Facebook" asociada al usuario logado.

4) Según consta en diligencia de 28 de enero de 2021, con fecha 21 y 22 de enero 2021 se comprobó en internet el contenido de:

a) La url ***URL.3 donde constaba:

"Condiciones de las Herramientas para empresas de Facebook.
[…]
ii. "Datos de eventos": información adicional que compartes sobre las personas y las acciones que estas realizan en tus sitios web, aplicaciones o tiendas, como visitar tus sitios web, instalar tus aplicaciones y comprar tus productos. Aunque los Datos de eventos incluyen información recopilada y transferida cuando las personas acceden a un sitio web o una aplicación mediante el inicio de sesión con Facebook o los plugins sociales (por ejemplo, el botón "Me gusta"), no incluyen información creada cuando una persona interactúa con nuestra plataforma a través del inicio de sesión con Facebook, mediante los plugins sociales o de cualquier otro modo (por ejemplo, al iniciar sesión, indicar que le gusta un artículo o una canción, o compartirlos). La información creada cuando una persona interactúa con nuestra plataforma a través del inicio de sesión con Facebook, mediante los plugins sociales o de cualquier otro modo está sujeta a las Condiciones de la plataforma.
[…]
2. Uso de los Datos de herramientas para empresas
a. En función de las Herramientas para empresas de Facebook que decidas usar, utilizaremos los Datos de herramientas para empresas con los siguientes fines: i. Información de contacto para la búsqueda de coincidencias
1. Nos indicas que tratemos la Información de contacto únicamente para establecer correspondencias con los identificadores de usuario ("Identificadores de usuario coincidentes"), así como para vincular estos identificadores con los Datos de eventos correspondientes. Eliminaremos la Información de contacto tras finalizar el proceso de búsqueda de coincidencias.
ii. Datos de eventos para servicios de medición y análisis

1. Puedes indicarnos que tratemos los Datos de eventos para (a) elaborar informes en tu nombre sobre la repercusión de tus campañas publicitarias y otro tipo de contenido en internet ("Informes de campaña") y (b) generar análisis y estadísticas sobre las personas y el uso que hacen de tus aplicaciones, sitios web, productos y servicios ("Análisis").

2. Te concedemos una licencia no exclusiva e intransferible para utilizar los Informes de campaña y los Análisis solo con fines empresariales internos y únicamente de forma anónima y global para objetivos relacionados con la medición. No divulgarás los Informes de campaña ni los Análisis (ni ninguna parte de ellos) a terceros, salvo que cuentes con nuestro consentimiento por escrito. No divulgaremos los Informes de campaña ni los Análisis (ni ninguna parte de ellos) a terceros sin tu permiso, salvo que (i) se hayan integrado con Informes de campaña y Análisis de varios terceros y (ii) se haya eliminado tu información de identificación de dichos documentos integrados.

iii. Datos de eventos para segmentar tus anuncios

1. Puedes proporcionar Datos de eventos para dirigir campañas publicitarias a las personas que interactúen con tu empresa. Puedes solicitarnos que creemos audiencias personalizadas, que son grupos de usuarios de Facebook basados en Datos de eventos, para dirigir campañas publicitarias (incluidas audiencias personalizadas del sitio web, audiencias personalizadas de aplicaciones para móviles y audiencias personalizadas fuera de internet). Facebook tratará los Datos de eventos a fin de crear dichas audiencias para ti. No puedes vender ni transferir estas audiencias, ni autorizar a terceros para que las vendan o transfieran. Facebook no proporcionará dichas audiencias a otros anunciantes, a menos que tú o tus proveedores de servicios compartáis audiencias con otros anunciantes mediante herramientas que ofrezcamos para tal fin, conforme a las restricciones y los requisitos de tales herramientas y nuestras condiciones.

2. Estas condiciones se aplican al uso de audiencias personalizadas del sitio web, audiencias personalizadas de la aplicación para móviles y audiencias personalizadas fuera de internet que se hayan creado mediante las Herramientas para empresas de Facebook. Las audiencias personalizadas a partir de una lista de clientes que se proporcionen mediante nuestra función independiente de audiencias personalizadas están sujetas a las Condiciones de las audiencias personalizadas a partir de una lista de clientes.

iv. Datos de eventos para enviar mensajes comerciales y sobre transacciones

1. Podemos usar los Identificadores de usuario coincidentes y los Datos de eventos asociados con el fin de ayudarte a ponerte en contacto con las personas mediante mensajes comerciales y sobre transacciones en Messenger y otros productos de las empresas de Facebook.

v. Datos de eventos para mejorar la entrega de anuncios, personalizar funciones y contenido, y mejorar y proteger los productos de Facebook

1. Puedes proporcionar Datos de eventos para mejorar la segmentación de anuncios y la optimización de entrega de campañas publicitarias. Podemos establecer una correlación entre esos Datos de eventos y las personas que usan los productos de las empresas de Facebook para respaldar los objetivos de tu campaña publicitaria, mejorar la eficacia de los modelos de entrega de anuncios y determinar la relevancia de los anuncios para las personas. Es posible que utilicemos los Datos de eventos para personalizar las funciones y el contenido (incluidos los anuncios y las recomendaciones) que mostramos a las personas dentro y fuera de los productos de las empresas de Facebook. En lo que respecta a la segmentación de anuncios y la optimización de la entrega, (i) utilizaremos los Datos de eventos para la optimización de la entrega solo tras incorporarlos a datos obtenidos de otros anunciantes o a información que se haya recopilado de los productos de Facebook, y (ii) no permitiremos a otros anunciantes ni a terceros mostrar publicidad basándose únicamente en los Datos de eventos.

2. Asimismo, a fin de mejorar la experiencia para las personas que usan productos de las empresas de Facebook, es posible que usemos los Datos de eventos para fomentar la seguridad y protección dentro y fuera de los productos de las empresas de Facebook, con fines de investigación y desarrollo, y para mantener la integridad de dichos productos y mejorarlos.

[…]

4. Modificación, rescisión y retención.

[…]

b. Con arreglo a las presentes condiciones, podemos conservar los Datos de eventos durante un período máximo de dos años. Conservaremos cualquier audiencia que hayas creado usando estos datos hasta que los elimines por medio de las herramientas de tu cuenta.[…]

[…]

5. Otras condiciones para el tratamiento de Información personal

a. En la medida en que los Datos de herramientas para empresas contengan Información personal que trates conforme al Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) (el 'RGPD"), se aplican las siguientes condiciones:

i. Las Partes reconocen y aceptan que tú eres el Controlador con respecto al Tratamiento de Información personal en los Datos de herramientas para empresas con el fin de proporcionar los servicios de coincidencias, medición y análisis descritos anteriormente en las secciones 2.a.i y 2.a.ii (por ejemplo, para proporcionarte Análisis e Informes de campaña), y que solicitas a Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublín 2 Irlanda ("Facebook Ireland") el Tratamiento de dicha Información personal con ese fin y en tu nombre, como

Procesador de conformidad con estas Condiciones de las herramientas para empresas de Facebook y las Condiciones del tratamiento de datos de Facebook. Las Condiciones del tratamiento de datos se incorporan de forma expresa y mediante esta referencia a las presentes Condiciones de las herramientas para empresas, y se aplican entre tú y Facebook Ireland junto con las presentes Condiciones de las herramientas para empresas.

ii. En cuanto a la Información personal en Datos de eventos relacionada con las acciones de las personas en tus sitios web y aplicaciones que integren las Herramientas para empresas de Facebook para cuyo Tratamiento tú y Facebook Ireland determinéis de forma conjunta los medios y fines, tú y Facebook Ireland reconocéis y aceptáis ser Cocontroladores de conformidad con el artículo 26 del RGPD. La corresponsabilidad abarca la recopilación de dicha Información personal mediante las Herramientas para empresas de Facebook y su posterior transmisión a Facebook Ireland, con el fin de usarla para los fines establecidos anteriormente en las secciones 2.a.iii a 2.a.v.1 ("Tratamiento conjunto"). Para obtener más información, haz clic aquí. El Tratamiento conjunto está sujeto al Apéndice para controladores, que se incorpora de forma expresa aquí mediante esta referencia a las presentes Condiciones de las herramientas para empresas, y se aplica entre tú y Facebook Ireland junto con las presentes Condiciones de las herramientas para empresas. Facebook Ireland sigue siendo Controlador independiente de conformidad con el artículo 4(7) del RGPD respecto del Tratamiento de dichos datos que se lleve a cabo después de que se transmitan a Facebook Ireland.

iii. Tú y Facebook Ireland seguís siendo, según corresponda en cada caso, Controladores independientes de conformidad con el artículo 4(7) del RGPD en cuanto al Tratamiento de Información personal en Datos de herramientas para empresas en virtud del RGPD que no esté sujeta a las secciones 5.a.i y 5.a.ii.

[…]"

b) En la url ***URL.5 constaba:

"Apéndice sobre transferencia de datos de la UE de Facebook

Este Apéndice sobre transferencia de datos de la UE ("Apéndice transferencia de datos") se aplica en la medida en que FIL actúe como Procesador de Datos de la UE de conformidad con las condiciones del producto aplicables, como las Condiciones de las herramientas para empresas de Facebook o las Condiciones de las audiencias personalizadas a partir de una lista de clientes ("Condiciones del producto aplicables"), y las transferencias de los Datos de la UE que se originen en el Reino Unido, la UE, el EEE o Suiza se realicen a su subprocesador Facebook, Inc.

1. Teniendo en cuenta las circunstancias, indicas a FIL que transfiera los Datos de la UE a Facebook, Inc. en los Estados Unidos para su almacenamiento y un Tratamiento más extenso. Las Cláusulas se aplican entre tú y Facebook, Inc. en relación con las transferencias de los Datos de la UE que se originen en el

Reino Unido, la Unión Europea, el Espacio Económico Europeo o Suiza a Facebook, Inc., a menos que en el RGPD se permitan de otro modo.

a. Respecto a las Cláusulas, tú eres el "exportador de datos" y Facebook, Inc. es el "importador de datos", de acuerdo con la definición de estos términos en dichas Cláusulas.

[…]

8. En este Apéndice sobre transferencia de datos:

a. "Cláusulas" hace referencia a las cláusulas tipo de protección de datos para la transferencia de datos personales a los procesadores establecidos en terceros países que no garanticen un nivel de protección de los datos adecuado, según se describe en el artículo 46 del RGPD y de acuerdo con la aprobación de la Decisión 2010/87/CE de la Comisión Europea del 5 de febrero de 2010 (pero sin incluir las cláusulas ilustrativas opcionales).

[…]"

c) En la url ***URL.6 constaba:

"Condiciones del tratamiento de datos

Aceptas que el uso que hagas de determinados Productos de Facebook puede implicar el envío de Información personal a Facebook. Las presentes Condiciones del tratamiento de datos se aplican en la medida en que se estipule que debemos tratar Información personal en calidad de Procesador en las condiciones de productos aplicables ("Condiciones de productos aplicables", y cualesquiera productos de Facebook a los que estas afecten, "Productos aplicables"), como las Condiciones de las herramientas para empresas de Facebook y las Condiciones de las audiencias personalizadas a partir de una lista de clientes

[…]

I0. Aceptas que Facebook pueda subcontratar las obligaciones que tiene conforme a las presentes Condiciones del tratamiento de datos a un subprocesador que pueda tener su sede en los Estados Unidos, la Unión Europea (UE), el Espacio Económico Europeo (EEE) u otros países, siempre que sea mediante un acuerdo escrito con dicho subprocesador en el que se le impongan obligaciones que sean como mínimo igual de estrictas que las que se imponen a Facebook en las presentes Condiciones del tratamiento de datos. Si el subprocesador no cumpliese estas obligaciones, Facebook asumirá ante ti plena responsabilidad por el ejercicio de las obligaciones del subprocesador.

[…]

12. En la medida en que el RGPD se aplique al Tratamiento que hagas como Controlador según estas Condiciones del tratamiento de datos, el Apéndice sobre transferencia de datos, que forma parte de dichas Condiciones y queda incorporado a estas por la presente referencia, será de aplicación a las transferencias de Información personal que se originen en Reino Unido, la UE, el EEE o Suiza."

d) En la url ******URL.7*** constaba, con fecha de entrada en vigor el 31 de agosto de 2020:

"Apéndice para controladores

El presente Apéndice para controladores se aplica cuando se incorpora de forma expresa por referencia a las condiciones de productos de Facebook, como en el caso de las Condiciones de las herramientas para empresas de Facebook (cualesquiera dichas condiciones, las "Condiciones de productos aplicables", y todos los productos de Facebook cubiertos, los "Productos aplicables"). Los términos en mayúsculas empleados en el presente Apéndice para controladores que no se definan en el mismo tienen los significados que se establecen en las Condiciones de productos aplicables. En caso de conflicto entre las Condiciones de productos aplicables y este Apéndice para controladores prevalecerá el segundo, solo en lo referente al ámbito de dicho conflicto.

Facebook y tú acordáis lo siguiente:

FIL, 4 Grand Canal Square, Grand Canal Harbour, Dublín 2, Irlanda ("Facebook Ireland" 0 "nosotros") y tú (cada uno, una "Parte" y, conjuntamente, las "Partes") sois Cocontroladores (de conformidad con el artículo 26 del RGPD) del Tratamiento conjunto especificado en las Condiciones de productos aplicables. El ámbito del Tratamiento conjunto y el presente Apéndice para controladores abarca la recopilación de los Datos personales especificados en las Condiciones de productos aplicables y su transmisión a Facebook Ireland. El tratamiento posterior de los datos por parte de Facebook Ireland no forma parte del Tratamiento conjunto. Puedes encontrar más información sobre el Tratamiento conjunto en las Condiciones de productos aplicables.

[…]

Para cumplir las obligaciones estipuladas en el RGPD en cuanto al Tratamiento conjunto, tus responsabilidades y las de Facebook Ireland se determinan a continuación:

N.º	Obligación conforme al RGPD	Facebook Ireland	Tú
1	Artículo 6: requisito de bases legales para el Tratamiento conjunto	X (en lo que respecta al tratamiento de Facebook Ireland)	X (en lo que respecta a tu tratamiento)
2	Artículos 13 y 14: proporcionar información sobre el Tratamiento conjunto de Datos personales		X Esto incluye, como mínimo, proporcionar la siguiente información además de tu política de datos estándar o documento similar: Informar de que Facebook Ireland es Cocontrolador del Tratamiento conjunto, y que la información requerida conforme al artículo 13(1)(a) y (b) del RGPD se puede encontrar en la Política de datos de Facebook Ireland en https://www.facebook.com/about/privacy. La especificación de la información que usas de los Productos aplicables, así como los fines de la recopilación y transmisión de Datos personales que constituyen el Tratamiento conjunto, se lleva a cabo tal y como se establece en las Condiciones de productos aplicables. Puede encontrarse más información sobre cómo Facebook Ireland trata los Datos personales, incluidas las bases legales en las que se basa Facebook Ireland y las formas de ejercer los derechos de las Personas interesadas contra Facebook Ireland, en la Política de datos de Facebook Ireland en https://www.facebook.com/about/privacy. Puedes encontrar más información sobre el Tratamiento conjunto en las Condiciones de productos aplicables.
3	Artículo 26(2): ofrecer información esencial relacionada con este Apéndice para controladores		X Esto incluye, como mínimo, proporcionar la siguiente información: Indicar que tú y Facebook Ireland: Habéis suscrito el presente Apéndice para controladores a fin de determinar las respectivas responsabilidades en cuanto al cumplimiento de las obligaciones que se estipulan en el RGPD con respecto al Tratamiento conjunto (como se especifica en las Condiciones de productos aplicables). Habéis aceptado que sois responsables de proporcionar a las Personas interesadas, como mínimo, la información descrita en el punto n.º 2. Habéis aceptado que, entre las Partes, Facebook Ireland es responsable de permitir los derechos de las Personas interesadas de conformidad con los artículos 15 a 20 del RGPD en lo que respecta a los Datos personales que Facebook Ireland almacena tras el Tratamiento conjunto.
4	Artículos 15 a 20: derechos de las Personas interesadas en lo que respecta a los Datos personales que Facebook almacena tras el Tratamiento conjunto	X	
5	Artículo 21: derecho de oposición, en la medida en que el Tratamiento conjunto se base en el artículo 6(1)(f)	X (en lo que respecta al tratamiento de Facebook Ireland)	X (en lo que respecta a tu tratamiento)
6	Artículo 32: seguridad del Tratamiento conjunto	X (en lo que respecta a la seguridad de los Productos aplicables)	X (en lo que respecta a la correcta implementación técnica y la configuración de los Productos aplicables)
7	Artículos 33 y 34: Vulneraciones de la seguridad de los datos personales en relación con el Tratamiento conjunto	X (en la medida en que la Vulneración de la seguridad de los datos personales esté relacionada con las obligaciones de Facebook Ireland de conformidad con el presente Apéndice para controladores)	X (en la medida en que la Vulneración de la seguridad de los datos personales esté relacionada con tus obligaciones de conformidad con el presente Apéndice para controladores)

El resto de las responsabilidades en cuanto al cumplimiento de las obligaciones estipuladas en el RGPD en lo que respecta al Tratamiento conjunto corresponden a cada Parte individualmente.
[…]"

e) En la url ******URL.8*** constaba:

"[…]
Autenticación
Utilizamos cookies para verificar tu cuenta y determinar si has iniciado sesión, con el objetivo de ayudarte a acceder a los productos de Facebook y mostrarte la experiencia y las funciones adecuadas.
Por ejemplo: utilizamos cookies para mantener tu sesión abierta mientras navegas entre páginas de Facebook. Las cookies también nos ayudan a

recordar tu navegador, de tal modo que no tengas que iniciar sesión en Facebook constantemente y puedas hacerlo fácilmente a través de aplicaciones y sitios web de terceros. Por ejemplo, utilizamos las cookies "c_user" y "xs" con este fin, con una duración de 365 días.
[…]
Publicidad, recomendaciones, estadísticas y medición
Utilizamos cookies para mostrar anuncios de empresas y otras organizaciones, y recomendarlas a personas que puedan estar interesadas en los productos, los servicios o las causas que promocionen dichas empresas.
Por ejemplo: las cookies nos permiten mostrar anuncios a personas que hayan visitado anteriormente el sitio web de una empresa, comprado sus productos o utilizado sus aplicaciones, y recomendarles productos y servicios en función de esa actividad. Así mismo, nos permiten limitar el número de veces que se muestra un anuncio, de tal modo que no veas el mismo una y otra vez. Por ejemplo, la cookie "fr" se usa para mostrar, medir y mejorar la relevancia de anuncios, y tiene una duración de 90 días.
También utilizamos cookies para medir el rendimiento de las campañas publicitarias de empresas que utilizan los productos de Facebook.
Por ejemplo: utilizamos cookies para contar el número de veces que se muestra un anuncio y calcular su coste. También usamos cookies para medir la frecuencia con que las personas llevan a cabo determinadas acciones, como efectuar una compra tras recibir un anuncio. La cookie "_fbp" identifica los navegadores para proporcionar servicios publicitarios y de análisis de sitios web, y tiene una duración de 90 días.
Las cookies nos ayudan a mostrar y medir anuncios en diferentes navegadores y dispositivos utilizados por la misma persona.
Por ejemplo: podemos utilizar cookies para impedir que veas el mismo anuncio una y otra vez en los diferentes dispositivos que utilices.
[…]"

f) En la url ******URL.9*** constaba:

"[…]
What data does the Facebook pixel collect?
See our Cookie Policy for details about the cookies used and the data received. The Facebook pixel receives these types of data:
• Http Headers - Anything present in HTTP headers. HTTP Headers are a standard web protocol sent between any browser request and any server on the internet. HTTP Headers include IP addresses, information about the web browser, page location, document, referrer and person using the website.
• Pixel-specific Data - Includes Pixel ID and the Facebook Cookie.
• Button Click Data - Includes any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks.
• Optional Values - Developers and marketers can optionally choose to send additional information about the visit through conversion tracking. Example custom data events are conversion value, page type, and more.
• Form Field Names — Includes website field names like 'email', 'address', 'quantity' for when you purchase a product or service. We don't capture field values unless you include them as part of Advanced Matching, or conversion tracking.
[…]"

De su traducción no oficial del inglés:
"[...]
¿Qué datos recoge el píxel de Facebook?
Consulte nuestra política de Cookie para obtener más información sobre las cookies utilizadas y los datos recibidos. El píxel de Facebook recibe estos tipos de datos:
• Http Headers — Todo presente en cabezas HTTP. Http Headers es un protocolo web estándar enviado entre cualquier solicitud de navegador y cualquier servidor de internet. Http Headers incluye las direcciones IP, la información sobre el navegador, la ubicación de la página, el documento, el remitente y la persona que utiliza el sitio web.
• Datos específicos de Pixel — Incluye el ID de Pixel y el Cookie de Facebook.
• Botón Click Data — Incluye los botones pulsados por los visitantes del sitio, las etiquetas de dichos botones y las páginas visitadas a raíz del botón.
• Valores opcionales — Los desarrolladores y comercializadores pueden optar por enviar información adicional sobre la visita a través del seguimiento de la conversión. Ejemplos de eventos de datos personalizados son el valor de conversión, el tipo de página, etc.
• Nombres de campo del formulario — Incluye nombres de campo del sitio web como «correo electrónico», «dirección», «cantidad» para la compra de un producto o servicio. No recogemos los valores de los campos a menos que los incluya como parte de Advanced Matching, o el seguimiento de la conversión.
[...]"

g) En la url ***URL.4 constaba:

Herramientas de Facebook para empresas

En la siguiente tabla se ofrece una descripción general sobre la Información personal que se recopila y transmite a Facebook Ireland como parte del Tratamiento conjunto al usar las Herramientas para empresas de Facebook. Sin embargo, ten en cuenta que la Información personal recopilada y transmitida también depende de tu configuración de las Herramientas para empresas de Facebook. Para obtener información más detallada, consulta la respectiva documentación para desarrolladores de las Herramientas para empresas de Facebook.

Datos de eventos --- Herramientas para empresas	Información del encabezado HTTP, que incluye datos sobre el navegador web o la aplicación usados (por ejemplo, el agente de usuario o la configuración regional de país o idioma)	Información relativa a los eventos estándar u opcionales, como "Visita a la página" o "Descarga de la aplicación", y otras propiedades del objeto, así como botones en los que los visitantes del sitio web hicieron clic, cada uno conforme a la configuración de la Herramienta para empresas	Identificadores en internet, incluidas direcciones IP y, en la medida en que se proporcionen, identificadores relacionados con Facebook o identificadores de dispositivos (por ejemplo, identificadores publicitarios para sistemas operativos de móvil), así como información sobre el estado de seguimiento de anuncios limitado o desactivado
Plugins sociales https://developers.facebook.com/docs/plugins/	x	-	x
Píxel https://developers.facebook.com/docs/facebook-pixel/	x	x	x
SDK de Facebook para eventos de la aplicación https://developers.facebook.com/docs/app-events/	x	x	x
Inicio de sesión (web/SDK) https://developers.facebook.com/docs/facebook-login/	x	-	x

Fecha de entrada en vigor: 31 de agosto de 2020

5) Según consta en diligencia de 16 de abril de 2021, con fecha 15 de abril de 2021 se comprobó que sin estar logado en Facebook y tras visitar la página ***URL.1,

aceptando sus cookies, constaban peticiones http GET y POST enviadas al dominio facebook.com con, entre otra, la siguiente información:

1. El valor de la cookie fbp enviado como parámetro dentro de la url.
2. parámetros sw, sh.
3. campo “accept-language”
4. campo “user-agent”
5. parámetro dl con el valor ***URL.1

Se comprobó asimismo que exclusivamente por realizar la operación de login en la cuenta de Facebook en facebook.com usando un usuario de prueba, se instalaban en el navegador cookies, entre otras, c_user, fr.

También con fecha 15 de abril de 2021, se comprobó que estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, constaban peticiones http GET y POST enviadas al dominio facebook.com con, entre otra, la siguiente información:

1. cookies c_user y fr entre otras. El valor de la cookie fbp enviado como parámetro dentro de la url.
2. parámetros sw, sh.
3. campo “accept-language”
4. campo “user-agent”
5. parámetro dl con el valor ***URL.1

6) Como consecuencia del requerimiento de información efectuado por la SGID, con fecha 17 de mayo de 2021 la parte reclamada remitió a esta Agencia la siguiente información y manifestaciones:

1. Que se había eliminado el Pixel de Facebook del código de las distintas webs bajo el dominio de la parte reclamada.
2. Que se aportaba el tráfico dirigido a la web de la parte reclamada desglosado por país de procedencia y durante el periodo en el periodo desde el 11 de abril a 10 de mayo de 2021. En dicho tráfico constaban, entre otras:
   - Para la web *****URL.1** países de procedencia como ***(…)***.
   - Para la web ******URL.1*** constan entre los países de procedencia ***(…).***
   - Para ******URL.10*** constan entre los países de procedencia ***(…).***
   - Para ******URL.10*** constan entre los países de procedencia ***(…).***

7) Como consecuencia del requerimiento de información efectuado por la Inspección, con fecha 04 de junio de 2021 la parte reclamada remitió a esta Agencia la siguiente información y manifestaciones:

1. Que la parte reclamada estaba localizada al 100% en España.
2. Que todos sus trabajadores y medios materiales estaban localizados en España.

QUINTO: Con fecha 5 de octubre de 2021 la labor del grupo de trabajo TF101 no había concluido, razón por la que se declaró la caducidad de las actuaciones previas de investigación al haber transcurrido más de doce meses desde su inicio, abriéndose a continuación nuevas actuaciones de investigación al no haber prescrito la infracción. Todas las actuaciones de investigación realizadas se han incorporado a la documentación obrante en ese nuevo procedimiento.

SEXTO: La Subdirección General de Inspección de Datos continuó con la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, teniendo conocimiento de los siguientes extremos:

1) Como consecuencia del requerimiento de información efectuado por la Inspección, con fecha 17 de enero de 2022 la parte reclamada remitió a esta Agencia la siguiente información y manifestaciones:

a. Que el modo en el que se determinaban los fines y medios antes de la retirada de Facebook Pixel de las web de la parte reclamada era:

> *"[…]*
> *Pese a que Facebook se autodenomina interesadamente como "encargado de tratamiento" respecto a los tratamientos de datos previstos en la estipulación 5.a.i de las "Condiciones de Tratamiento" de Facebook, entendemos que la calificación jurídica correcta es que Freepik era corresponsable junto con Facebook en relación con los tratamientos de datos producidos en relación con los apartados 2.a.i y 2.a.ii de las Condiciones de Herramientas.*
> *Respecto a la elección sobre los fines, Freepik y Facebook determinaban en el pasado conjuntamente la finalidad que era medir el resultado de las acciones integrantes de una determinada campaña, realizadas por las personas impactadas por la misma.*
> *Con respecto a la elección sobre los medios, Facebook decide y preconfigura hasta 18 opciones de eventos en su consola de control. Freepik únicamente seleccionaba aquellos que consideraba que necesitaba estrictamente para obtener la visibilidad de resultados de sus campañas. Es importante resaltar que Freepik tenía la posibilidad, pero no creó eventos diferentes, y únicamente seleccionó 5 de esos 18 eventos, para obtener información agregada sobre cuáles de dichos eventos seleccionados eran realizados por las personas impactadas por la campaña. Es decir, Freepik limitó sustancialmente el alcance de sus tratamientos, dentro de los parámetros previstos por Facebook.*
> *[…]"*

Y posteriormente añadía:

> *"[…]*
> *En cuanto a la determinación de los fines, Freepik y Facebook determinaban conjuntamente la finalidad del tratamiento, que es mostrar un anuncio específico a un conjunto de personas (la audiencia personalizada) que constituía el público objetivo de cada campaña.*
> *En lo que respecta a la determinación de los medios, Freepik y Facebook determinaban conjuntamente los medios para la segmentación de dicha audiencia. Freepik, participaba en la determinación de los medios eligiendo utilizar parte de los servicios ofrecidos por Facebook y solicitándole que impactara a una audiencia personalizada en función de determinados criterios. Facebook, por su parte, había decidido tratar los datos personales de sus usuarios perfilándolos de acuerdo con múltiples criterios que ponía a disposición de Freepik. En este sentido, Facebook ya había diseñado los medios esenciales del tratamiento (como las categorías de datos objeto de tratamiento, los criterios de selección ofrecidos y quién tendrá acceso (y a qué) datos personales en el contexto de cada campaña concreta.*

[…]"

b. Que en relación a la inserción y utilización de Facebook Login en sus webs, la parte reclamada y FACEBOOK eran corresponsables.

Y manifestaba:

"[…]
Freepik y Facebook son corresponsables en relación con la inserción y utilización del Facebook login en las webs de Freepik.
En cuanto a los tratamientos de datos relacionados con el Facebook Login, Freepik decide integrarlo en su web para delegar en Facebook la tarea de identificar a los usuarios que lo utilicen. Los beneficios para Freepik (y para los usuarios) son evidentes, desde el punto de vista de (i) "user experience" pues facilita el primer acceso (registro) y sucesivos como usuario registrado de Freepik a usuarios registrados en Facebook sin apenas fricción, y (ii) de seguridad, pues el usuario no tiene que crear contraseñas ad hoc, y Freepik no tiene que almacenarlas ni asumir el riesgo de su pérdida o acceso por parte de terceros no autorizados.
A título de ejemplo, en nuestra propia experiencia, el registro federado permitió limitar de forma sustancial las consecuencias de la brecha de seguridad comunicada a esta Agencia el día 29 de junio de 2020, en la que un atacante externo pudo acceder a las direcciones de correo electrónico de 8.3M de usuarios. De dicha cifra de usuarios afectados por dicha brecha, más de la mitad (4,5M) tenían su cuenta federada con FACEBOOK u otra plataforma, por lo que el atacante únicamente pudo acceder a su dirección de correo.
En relación con los medios, son decididos conjuntamente al insertar Freepik en el código de sus webs el botón de login, que, al ser pulsado por el usuario, activa el procedimiento de registro en la ventana modal de Facebook.
Freepik limita su responsabilidad al regular funcionamiento del botón incrustado en sus webs, dentro de las opciones habilitadas por Facebook, y a minimizar el perímetro del tratamiento de datos personales en el proceso. Cabe insistir en que Facebook no obtiene datos personales adicionales nuevos, más allá del registro de la fecha y hora en que cada usuario registrado común accede a Freepik.
[…]"

b. Que en relación a cómo se informaba a los interesados de las respectivas responsabilidades según art. 26 RGPD manifestaba que en la "ventana modal" de "Facebook Login" controlada por FACEBOOK se informaban de los tratamientos realizados por ambos corresponsables.

Aporta captura de pantalla donde se veía la ventana de Facebook Login donde el usuario debía introducir usuario y contraseña y a continuación constaba "*Si continúas, Freepik Company tendrá acceso continuo a la información que compartes y Facebook registrará cuando Freepik Company acceda a ella. Más información sobre estos datos que compartes y tu configuración. Política de Privacidad y Condiciones de Freepik Company*." donde las palabras "*Más información*", "*Política de privacidad"* y "*Condiciones"* son hiperenlaces.

Y manifestó que en el enlace del servicio web archive ******URL.11*** constaba:

"[…]
Además Freepik contrata servicios de publicidad personalizada de diversas plataformas de social media (como Facebook y otros) para atraer a nuestra web a potenciales nuevos usuarios que han sido perfilados por dichas plataformas de acuerdo con sus intereses. Freepik selecciona, entre esos perfiles, a los que entendemos que pueden estar interesados en nuestros productos (por ejemplo, los usuarios que ya han visitado nuestras webs o aquellos usuarios de una determinada franja de edad o localización geográfica).
Estas plataformas integran "cookies" y otras tecnologías (de Facebook por ejemplo) en nuestra web que, -previo tu consentimiento a su uso-, les permiten observar, por ejemplo si sus usuarios sólo han accedido a la web de Freepik y la han abandonado sin más, o han descargado productos o se han convertido en usuarios Premium.
Después nos suministran esa información de forma agregada y anónima para facturarnos en consecuencia, lo que nos permite entender mejor la rentabilidad de nuestras campañas publicitarias en cada plataforma.
Además, podemos mostrar anuncios a los visitantes que hayan abandonado nuestra web p.ej. sin registrarse, para intentar terminar de convencerles de que lo hagan (remarketing).
En relación con estos tratamientos de datos, Freepik es "corresponsable" junto con cada una de dichas plataformas, en relación con (i) la selección de los intereses de sus usuarios a quienes pedimos que muestre nuestra publicidad; (ii) su seguimiento y observación en nuestra web; y (iii) el suministro de datos estadísticos y agregados a Freepik sobre el resultado de estas campañas, es decir, la conversión, en su caso, en clientes nuestros.
Todos estos tratamientos se realizan sin que Freepik pueda identificarte: sólo te identificamos cuando te registras como usuario gratuito o premium.
Por lo demás, Freepik no participa o se responsabiliza de los tratamientos realizados por los anunciantes y plataformas citadas para sus propias finalidades, de forma previa o posterior a los tratamientos realizados en conjunto con Freepik. Freepik está adherida al acuerdo standard de Corresponsabilidad de Facebook, en cuya virtud te hemos descrito el alcance de nuestros tratamientos compartidos, te suministramos el enlace a la política de privacidad de Facebook Ireland, donde esta informa de los aspectos legalmente obligatorios, y te informamos de que Facebook Ireland será la encargada de atender los derechos en materia de protección de datos (arts 15 a 20 Reglamento General de Protección de Datos) en lo relacionado con los datos personales almacenados por Facebook Ireland tras el tratamiento compartido.
[...]".

Y manifestaba que, en la actualidad, su información ya no hacía referencia a estos tratamientos en lo que se refería al Facebook Píxel, una vez suprimido.

c. Asimismo, manifestó, en lo que se refiere a Facebook Login, que su política de privacidad en la actualidad decía lo siguiente:

"Puedes abrir tu cuenta como Usuario registrado en Freepik con tu propia cuenta en otras plataformas, como por ejemplo Facebook, utilizando los Logins federados que encontrarás en la parte superior de nuestras webs, y acceder siempre que quieras a través de los mismos, sin necesidad de crear y recordar un nombre de usuario y contraseña específicas para acceder a Freepik.
Esta opción es posible gracias a la colaboración entre Freepik y estas plataformas como corresponsables conjuntos del tratamiento de tus datos personales, para que (i) puedas identificarte directamente en dichas plataformas, (ii) estas nos confirmen que eres quien dices ser, y (iii) nosotros te facilitemos tu ingreso como usuario registrado en Freepik.
Freepik obtiene de estas plataformas, bajo tu consentimiento, tu nombre de usuario, imagen y tu dirección de correo electrónico con la finalidad de proceder a tu registro como usuario de Freepik. Estas plataformas captan identificadores online (dirección IP), identificadores técnicos (de tu dispositivo, así como sus identificadores publicitarios como "google id" o "apple id") y registran, cada vez que utilizas su login, la fecha y hora de tu acceso a Freepik.
Puedes ejercer tus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y revocación del consentimiento relacionados con los datos personales obtenidos de estas plataformas (y otros que hayas podido facilitar a Freepik en tu relación con nosotros) dirigiéndote a Freepik en la dirección de correo electrónico suministrada en esta misma política.
¡Ojo! La rectificación o supresión de tus datos en tu cuenta de Freepik, no implica automáticamente la rectificación o supresión de tus datos y cuentas de las plataformas que autentiquen tu identidad: deberás dirigirte también a ellas para ejercer tus derechos.
Para ejercer tus derechos en materia de protección de datos personales en relación con cualesquiera otros datos derivados de tu relación con estas plataformas deberás dirigirte a la plataforma correspondiente.
Puedes obtener información adicional en los siguientes enlaces:
1. Facebook:
Apéndice para responsables y corresponsables de tratamiento de Facebook (disponible en este enlace).
Política de privacidad de Facebook en este enlace. (...)"

d. Que en respuesta a cuál era el contrato celebrado con FIL o con FACEBOOK INC., de conformidad con el art. 28.3 RGPD, respondió que era el que se encontraba en la dirección ***URL.6

e. Manifestó:
"[…]
consideramos que los identificadores y resto de información obtenida directamente del usuario a través del Facebook login (tal y como se ha descrito en la respuesta anterior) son indudablemente datos personales, porque son objeto de captación y tratamiento y se añaden al resto de datos personales de cada usuario registrado —identificado, por tanto- de Facebook.
[…]"

f. Que de acuerdo con el "Apéndice sobre transferencia de datos de ciudadanos europeos de Facebook" aplicable desde el 27 de septiembre de 2021 la transferencia de datos a Estados Unidos se basaba en:

a. Cláusulas contractuales tipo (2010) entre responsable (Facebook Ireland) y encargado (Facebook Inc). (Cláusula 6.c) del apéndice).
b. Cláusulas contractuales tipo (2021 P2P o entre encargados de tratamiento) entre las filiales del grupo Facebook. (Cláusula 6.i) del apéndice).

g. Respecto a la existencia de transferencia internacional manifestó:
"[…]
Nos parece adecuado añadir que, atendidas las recientes Guidelines 5/2021 del EDPB, en este proceso no existe transferencia internacional de datos personales, en la medida en que el fluio de datos personales se realiza. no entre el sitio web de Freepik y el de Facebook, sino directamente entre el usuario de Facebook y Facebook„ por iniciativa de aquel. y a través de la ventana modal de Facebook (véase, mutatis mutandis, el ejemplo 1 descrito en la pág. 5 de dichas Guidelines).
Si existiera transferencia internacional de datos (y sostenemos que no existe), desde nuestro punto de vista la cuestión nuclear sería la posibilidad jurídica y probabilidad práctica de que las Agencias de inteligencia norteamericanas requirieran el acceso a precisamente ese histórico de datos de acceso a Freepik, únicos datos que Facebook obtiene como consecuencia del funcionamiento del Facebook Login en Freepik."

h. En respuesta a si se habían aplicado medidas complementarias por parte de la parte reclamada o de FACEBOOK manifestó:
"Seguimos considerando que, atendidas sus circunstancias, dicho flujo de datos (incluso aunque fuera considerado una transferencia internacional de datos) no requiere medida complementaria alguna en el sentido de las Recommendations 1/2020 del EDPB. Si existiera transferencia internacional de datos (y sostenemos que no existe), desde nuestro punto de vista la cuestión clave sería entonces la posibilidad jurídica y probabilidad práctica de que las Agencias de inteligencia norteamericanas requirieran formalmente el acceso a precisamente esos datos de acceso a Freepik, únicos datos que Facebook obtiene como consecuencia del funcionamiento del Facebook Login en nuestra web. Por los motivos que fueron argumentados ante esta Agencia en diciembre de 2020, consideramos que existen motivos objetivos para considerar que existe una probabilidad ínfima de que las Agencias de inteligencia norteamericanas requieran los datos tratados por Freepik."

i. Según consta en diligencia de 22 de marzo de 2022, con fecha 08 de febrero de 2022 se comprobó que estando logado en Facebook con un usuario de prueba, y tras visitar la página ***URL.1 aceptando todas sus cookies, no constaban peticiones http enviadas al dominio facebook.com ni facebook.net.

2) Según consta en diligencia de 26 de mayo de 2022, ese mismo día se comprobó que:

1. Las cookies cargadas en el navegador al realizar un login en Facebook con un usuario de prueba eran: presence, xs, c_user, fr, sb, datr todas instaladas por el dominio facebook.com.

2. Estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, no constaban peticiones http enviadas a ningún dominio con la palabra “facebook”.

3) Según consta en diligencia de 14 de septiembre de 2022, ese mismo día se comprobó que estando previamente logado en una cuenta de Facebook, al visitar la web ***URL.1 y hacer clic en el icono de Facebook para poder registrarse como usuario, se transmitían al domino facebook.com los siguientes datos, entre otros, dentro de una petición http POST:

1. cookies datr, sb, c_user, fr, xs, presence.
2. parámetro “accept-language”.
3. parámetro “user-agent:”
4. dentro del campo referer, la siguiente información:

(…).

4) Según consta en diligencia de 15 de septiembre de 2022, con fecha 05 de mayo de 2021 FIL remitió a la Autoridad Irlandesa de Protección de Datos (DPC), la siguiente información y manifestaciones, de su traducción no oficial del inglés:

(…).

Siendo su traducción no oficial al castellano:

(…).

c. Manifestó:

[…]

Siendo su traducción no oficial al castellano:

[…]

Con fecha 10 de septiembre de 2021 FIL remitió a la Autoridad Irlandesa de Protección de Datos (DPC), la siguiente información y manifestaciones:

a. Manifestó:

[…]

De su traducción no oficial del original en inglés a continuación:

[…]

Siendo su traducción no oficial al castellano:

[…]

Siendo su traducción no oficial al castellano:

[…]

De su traducción no oficial del original en inglés a continuación:

[…]

Con fecha 16 de mayo de 2022 META PLATFORMS INC (antigua FACEBOOK INC.) remitió a la Autoridad Austríaca de Protección de Datos (DSB), la siguiente información y manifestaciones, de su traducción no oficial del original en alemán, en relación principalmente a la herramienta FACEBOOK LOGIN. Dichas manifestaciones estaban contenidas en la transcripción del procedimiento oral mantenido entre la DSB y META PLATFORMS INC y había sido compartida por la DSB en el marco del grupo de trabajo TF101.

1. ***En relación a los roles: […].***

2. ***En relación a los datos tratados: […].***

SÉPTIMO: Con fecha 27 de octubre de 2022 la labor del grupo de trabajo TF101 no había concluido, razón por la que se declaró la caducidad de las actuaciones previas de investigación al haber transcurrido más de doce meses desde su inicio, abriéndose a continuación nuevas actuaciones de investigación al no haber prescrito la infracción. Todas las actuaciones de investigación realizadas se han incorporado a la documentación obrante en el presente procedimiento.

OCTAVO: En fecha 20 de julio de 2023 desde la Subdirección General de Inspección de Datos de esta Agencia se comprobó que FACEBOOK mantiene publicado en internet las solicitudes FISA que recibe.

NOVENO: Con fecha 17 de noviembre de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de apercibimiento a la parte reclamada, por la presunta infracción del Artículo 44 del RGPD, tipificada en el Artículo 83.4 del RGPD.

DÉCIMO: La notificación del citado acuerdo de iniciación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogida en fecha 20/11/2023 como consta en el acuse de recibo que obra en el expediente.

DÉCIMO PRIMERO: En fecha 30 de noviembre de 2023 se recibió escrito de alegaciones de la parte reclamada en el que, en síntesis, se recogen las siguientes consideraciones:

- Se mantiene en las consideraciones ya efectuadas en la fase de actuaciones previas de investigación
- La parte reclamada ha implementado los mecanismos jurídicos de transferencia y medidas más adecuados entre los disponibles en cada momento
- Desde la aprobación en los EEUU de Norteamérica y en la Unión Europea de los instrumentos normativos y de su aplicación a Meta Platforms Ireland Limited (antigua Facebook Ireland) y Meta Platforms Inc (antigua Facebook Platforms Inc), no existe infracción ni necesidad de imponerse por la Agencia ulteriores medidas de regularización.
- Entrada en vigor de nueva normativa relevante a ambos lados del Atlántico con la aprobación del "Trans-Atlantic Data Privacy Framework": Se estableció un sistema equivalente al preexistente en el Privacy Shield al que se añadieron nuevas garantías
- Aplicación del DPF a Facebook

DÉCIMO SEGUNDO: El 21 de febrero de 2024 la parte reclamada presentó un escrito ante esta Agencia en el que informaba que había decidido eliminar el inicio de sesión o "login federado" de Facebook como alternativa de acceso a los usuarios registrados del código de las distintas webs de Freepik. Y que esta eliminación se había hecho efectiva el día 9 de febrero de 2024.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes:

HECHOS PROBADOS

PRIMERO: El 2 de septiembre de 2020, en el plenario del Comité Europeo de Protección de datos se decidió crear un grupo de trabajo (en adelante, "TF101") para asegurar una aproximación coherente entre las autoridades de datos europeas para gestionar las 101 reclamaciones de NOYB, que versaban sobre cuestiones similares (quien reclamaba había visitado una página web de un responsable de tratamiento mientras había iniciado sesión en su cuenta de Google o Facebook, vinculada a su dirección de correo electrónico. Y el responsable de tratamiento había embebido código de servicios de Google o Facebook, que habían transferido sus datos personales a Estados Unidos, sin tener base jurídica para ello), según consta en la diligencia de fecha 25 de octubre de 2023.

SEGUNDO: "Facebook Connect" era la herramienta que, en su momento, permitía el registro de usuarios utilizando credenciales de FACEBOOK en lugar de crear un nombre de usuario y contraseña específicos para el servicio. Que a 11 de diciembre de 2020 se denominaba "Facebook Login", según se explica en el escrito de respuesta a requerimiento de la parte reclamada de esa fecha.

TERCERO: Las webs de la parte reclamada tenían incrustado el código de "Facebook Login" a 11 de diciembre de 2020, según se explica en el escrito de respuesta a requerimiento de la parte reclamada de esa fecha.

CUARTO: Las páginas web de la parte reclamada utilizaban “Facebook Login” como identidad federada, a 11 de diciembre de 2020, según se explica en el escrito de respuesta a requerimiento de la parte reclamada de esa fecha.

QUINTO: El funcionamiento de “Facebook Login” a 11 de diciembre de 2020 era el siguiente: cuando el usuario decidía crear su cuenta usando sus credenciales de FACEBOOK, y pulsaba el botón de la red social, se producía una llamada a la API de FACEBOOK, que abría una ventana en la que el usuario tenía que introducir su correo electrónico y contraseña de su cuenta de FACEBOOK para completar el proceso de registro. En dicha ventana, controlada por FACEBOOK, el usuario era informado de que FACEBOOK compartirá con FREEPIK ciertos datos para llevar a cabo el proceso de registro, tales como nombre, fotografía y dirección de correo electrónico. Y sólo cuando el interesado había prestado su consentimiento específico a este tratamiento, el proceso terminaba y la cuenta de usuario era creada en FREEPIK. FREEPIK recibía solamente el nombre de usuarios, cuenta de correo electrónico y fotografía del usuario). Todo ello según se explica en el escrito de respuesta a requerimiento de la parte reclamada de esa fecha.

SEXTO: A 11 de diciembre de 2020, dependiendo de la configuración, “Facebook Login”, permitía obtener, previa aprobación por el interesado, de una cantidad de datos personales de distinto alcance, como p.ej. el listado de amigos en FACEBOOK, las páginas a las que se ha dado a “like”, la localización o el género. En el caso de la parte reclamada, solo solicitaban y obtenían, previo consentimiento, los datos mínimos posibles: nombre de usuario, dirección de email y fotografía. Como campo obligatorio aparecían el nombre y la foto de perfil y, como campo opcional, la dirección de correo electrónico. Todo ello según se explica en el escrito de respuesta a requerimiento de la parte reclamada de esa fecha.

SÉPTIMO: A 11 de diciembre de 2020, el inicio de sesión estaba configurado para enviar información sobre el visitante directamente a FACEBOOK. FACEBOOK ofrecía un resumen de los datos tratados por sus productos en ***URL.4. El contrato que regía su relación con FACEBOOK se encontraba en ***URL.3 . Todo ello según se explica en el escrito de respuesta a requerimiento de la parte reclamada de 11 de diciembre de 2023.

OCTAVO: A 11 de diciembre de 2020, la transferencia internacional de datos personales entre la parte reclamada y FACEBOOK se basaba en el Apéndice sobre transferencia de datos de la UE ubicado en ***URL.5 . El modelo de cláusulas contractuales tipo utilizadas era el de la Comisión en 2010. Todo ello según se explica en el escrito de respuesta a requerimiento de la parte reclamada de 11 de diciembre de 2023.

NOVENO: A 11 de diciembre de 2020, la Foreign Intelligence Surveillance Act (FISA) permitía que se interceptaran las comunicaciones, contenidos, metadatos que se cruzaran entre potencias extranjeras agentes e instalaciones, con contenido relacionado materialmente con actividades ligadas a terrorismo, actos hostiles, armas de destrucción masiva, actividades clandestinas de espionaje, o con la defensa nacional, o actividades de asuntos exteriores de los EEUU. Con posterioridad a 2016, se ha restringido la capacidad de requerir, con base en la Sección 702, información basada en palabras clave a encontrar en el contenido de las comunicaciones (lo que

se aludía con requerimientos sobre "about") de modo que sólo se puede requerir información basada en identificadores ("selector") de la persona que emite o recibe la comunicación (lo que se alude como requerimientos "from" y/o "to"). Todo ello según se explica en el escrito de respuesta a requerimiento de la parte reclamada de 11 de diciembre de 2023.

DÉCIMO: El 22 de enero 2021 estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, dicha visita constaba en la sección “Actividad fuera de Facebook” asociada al usuario logado, según se recoge en la diligencia de 28 de enero de 2021.

DÉCIMO PRIMERO: El 21 y 22 de enero de 2021, según consta en diligencia de 28 de enero de 2021, en la url ***URL.3 constaba:

> *“Condiciones de las Herramientas para empresas de Facebook.*
> *[…]*
> *ii. "Datos de eventos": información adicional que compartes sobre las personas y las acciones que estas realizan en tus sitios web, aplicaciones o tiendas, como visitar tus sitios web, instalar tus aplicaciones y comprar tus productos. Aunque los Datos de eventos incluyen información recopilada y transferida cuando las personas acceden a un sitio web o una aplicación mediante el inicio de sesión con Facebook o los plugins sociales (por ejemplo, el botón "Me gusta"), no incluyen información creada cuando una persona interactúa con nuestra plataforma a través del inicio de sesión con Facebook, mediante los plugins sociales o de cualquier otro modo (por ejemplo, al iniciar sesión, indicar que le gusta un artículo o una canción, o compartirlos). La información creada cuando una persona interactúa con nuestra plataforma a través del inicio de sesión con Facebook, mediante los plugins sociales o de cualquier otro modo está sujeta a las Condiciones de la plataforma.*
> *[…]*
> *2. Uso de los Datos de herramientas para empresas*
> *a. En función de las Herramientas para empresas de Facebook que decidas usar, utilizaremos los Datos de herramientas para empresas con los siguientes fines: i. Información de contacto para la búsqueda de coincidencias*
> *1. Nos indicas que tratemos la Información de contacto únicamente para establecer correspondencias con los identificadores de usuario ("Identificadores de usuario coincidentes"), así como para vincular estos identificadores con los Datos de eventos correspondientes. Eliminaremos la Información de contacto tras finalizar el proceso de búsqueda de coincidencias.*
> *ii. Datos de eventos para servicios de medición y análisis*
> *1. Puedes indicarnos que tratemos los Datos de eventos para (a) elaborar informes en tu nombre sobre la repercusión de tus campañas publicitarias y otro tipo de contenido en internet ("Informes de campaña") y (b) generar análisis y estadísticas sobre las personas y el uso que hacen de tus aplicaciones, sitios web, productos y servicios ("Análisis").*

2. Te concedemos una licencia no exclusiva e intransferible para utilizar los Informes de campaña y los Análisis solo con fines empresariales internos y únicamente de forma anónima y global para objetivos relacionados con la medición. No divulgarás los Informes de campaña ni los Análisis (ni ninguna parte de ellos) a terceros, salvo que cuentes con nuestro consentimiento por escrito. No divulgaremos los Informes de campaña ni los Análisis (ni ninguna parte de ellos) a terceros sin tu permiso, salvo que (i) se hayan integrado con Informes de campaña y Análisis de varios terceros y (ii) se haya eliminado tu información de identificación de dichos documentos integrados.

iii. Datos de eventos para segmentar tus anuncios

1. Puedes proporcionar Datos de eventos para dirigir campañas publicitarias a las personas que interactúen con tu empresa. Puedes solicitarnos que creemos audiencias personalizadas, que son grupos de usuarios de Facebook basados en Datos de eventos, para dirigir campañas publicitarias (incluidas audiencias personalizadas del sitio web, audiencias personalizadas de aplicaciones para móviles y audiencias personalizadas fuera de internet). Facebook tratará los Datos de eventos a fin de crear dichas audiencias para ti. No puedes vender ni transferir estas audiencias, ni autorizar a terceros para que las vendan o transfieran. Facebook no proporcionará dichas audiencias a otros anunciantes, a menos que tú o tus proveedores de servicios compartáis audiencias con otros anunciantes mediante herramientas que ofrezcamos para tal fin, conforme a las restricciones y los requisitos de tales herramientas y nuestras condiciones.

2. Estas condiciones se aplican al uso de audiencias personalizadas del sitio web, audiencias personalizadas de la aplicación para móviles y audiencias personalizadas fuera de internet que se hayan creado mediante las Herramientas para empresas de Facebook. Las audiencias personalizadas a partir de una lista de clientes que se proporcionen mediante nuestra función independiente de audiencias personalizadas están sujetas a las Condiciones de las audiencias personalizadas a partir de una lista de clientes.

iv. Datos de eventos para enviar mensajes comerciales y sobre transacciones

1. Podemos usar los Identificadores de usuario coincidentes y los Datos de eventos asociados con el fin de ayudarte a ponerte en contacto con las personas mediante mensajes comerciales y sobre transacciones en Messenger y otros productos de las empresas de Facebook.

v. Datos de eventos para mejorar la entrega de anuncios, personalizar funciones y contenido, y mejorar y proteger los productos de Facebook

1. Puedes proporcionar Datos de eventos para mejorar la segmentación de anuncios y la optimización de entrega de campañas publicitarias. Podemos establecer una correlación entre esos Datos de eventos y las personas que usan los

productos de las empresas de Facebook para respaldar los objetivos de tu campaña publicitaria, mejorar la eficacia de los modelos de entrega de anuncios y determinar la relevancia de los anuncios para las personas. Es posible que utilicemos los Datos de eventos para personalizar las funciones y el contenido (incluidos los anuncios y las recomendaciones) que mostramos a las personas dentro y fuera de los productos de las empresas de Facebook. En Io que respecta a la segmentación de anuncios y la optimización de la entrega, (i) utilizaremos los Datos de eventos para la optimización de la entrega solo tras incorporarlos a datos obtenidos de otros anunciantes o a información que se haya recopilado de los productos de Facebook, y (ii) no permitiremos a otros anunciantes ni a terceros mostrar publicidad basándose únicamente en los Datos de eventos.

2. Asimismo, a fin de mejorar la experiencia para las personas que usan productos de las empresas de Facebook, es posible que usemos los Datos de eventos para fomentar la seguridad y protección dentro y fuera de los productos de las empresas de Facebook, con fines de investigación y desarrollo, y para mantener la integridad de dichos productos y mejorarlos.

5. Otras condiciones para el tratamiento de Información personal

a. En la medida en que los Datos de herramientas para empresas contengan Información personal que trates conforme al Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) (el 'RGPD"), se aplican las siguientes condiciones:

i. Las Partes reconocen y aceptan que tú eres el Controlador con respecto al Tratamiento de Información personal en los Datos de herramientas para empresas con el fin de proporcionar los servicios de coincidencias, medición y análisis descritos anteriormente en las secciones 2.a.i y 2.a.ii (por ejemplo, para proporcionarte Análisis e Informes de campaña), y que solicitas a Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublín 2 Irlanda ("Facebook Ireland") el Tratamiento de dicha Información personal con ese fin y en tu nombre, como Procesador de conformidad con estas Condiciones de las herramientas para empresas de Facebook y las Condiciones del tratamiento de datos de Facebook. Las Condiciones del tratamiento de datos se incorporan de forma expresa y mediante esta referencia a las presentes Condiciones de las herramientas para empresas, y se aplican entre tú y Facebook Ireland junto con las presentes Condiciones de las herramientas para empresas.

ii. En cuanto a la Información personal en Datos de eventos relacionada con las acciones de las personas en tus sitios web y aplicaciones que integren las Herramientas para empresas de Facebook para cuyo Tratamiento tú y Facebook Ireland determinéis de forma conjunta los medios y fines, tú y Facebook Ireland reconocéis y aceptáis ser Cocontroladores de conformidad con el artículo 26 del RGPD. La corresponsabilidad

abarca la recopilación de dicha Información personal mediante las Herramientas para empresas de Facebook y su posterior transmisión a Facebook Ireland, con el fin de usarla para los fines establecidos anteriormente en las secciones 2.a.iii a 2.a.v.1 ("Tratamiento conjunto"). Para obtener más información, haz clic aquí. El Tratamiento conjunto está sujeto al Apéndice para controladores, que se incorpora de forma expresa aquí mediante esta referencia a las presentes Condiciones de las herramientas para empresas, y se aplica entre tú y Facebook Ireland junto con las presentes Condiciones de las herramientas para empresas. Facebook Ireland sigue siendo Controlador independiente de conformidad con el artículo 4(7) del RGPD respecto del Tratamiento de dichos datos que se lleve a cabo después de que se transmitan a Facebook Ireland.
iii. Tú y Facebook Ireland seguís siendo, según corresponda en cada caso, Controladores independientes de conformidad con el artículo 4(7) del RGPD en cuanto al Tratamiento de Información personal en Datos de herramientas para empresas en virtud del RGPD que no esté sujeta a las secciones 5.a.i y 5.a.ii.
[…]"

DÉCIMO SEGUNDO: El 21 y 22 de enero de 2021, según consta en diligencia de 28 de enero de 2021, en la url ***URL.5 constaba:

"Apéndice sobre transferencia de datos de la UE de Facebook
Este Apéndice sobre transferencia de datos de la UE ("Apéndice transferencia de datos") se aplica en la medida en que FIL actúe como Procesador de Datos de la UE de conformidad con las condiciones del producto aplicables, como las Condiciones de las herramientas para empresas de Facebook o las Condiciones de las audiencias personalizadas a partir de una lista de clientes ("Condiciones del producto aplicables"), y las transferencias de los Datos de la UE que se originen en el Reino Unido, la UE, el EEE o Suiza se realicen a su subprocesador Facebook, Inc.
1. Teniendo en cuenta las circunstancias, indicas a FIL que transfiera los Datos de la UE a Facebook, Inc. en los Estados Unidos para su almacenamiento y un Tratamiento más extenso. Las Cláusulas se aplican entre tú y Facebook, Inc. en relación con las transferencias de los Datos de la UE que se originen en el Reino Unido, la Unión Europea, el Espacio Económico Europeo o Suiza a Facebook, Inc., a menos que en el RGPD se permitan de otro modo.
a. Respecto a las Cláusulas, tú eres el "exportador de datos" y Facebook, Inc. es el "importador de datos", de acuerdo con la definición de estos términos en dichas Cláusulas.
[…]
8. En este Apéndice sobre transferencia de datos:
a. "Cláusulas" hace referencia a las cláusulas tipo de protección de datos para la transferencia de datos personales a los procesadores establecidos en terceros países que no garanticen un nivel de protección de los datos adecuado, según se describe en el artículo 46 del RGPD y de acuerdo con la aprobación de la Decisión 2010/87/CE de la Comisión Europea del 5 de febrero de 2010 (pero sin incluir las cláusulas ilustrativas opcionales).

[…]”

DÉCIMO TERCERO: El 21 y 22 de enero de 2021, según consta en diligencia de 28 de enero de 2021, en la url ***URL.6 constaba:

> *“Condiciones del tratamiento de datos*
> *Aceptas que el uso que hagas de determinados Productos de Facebook puede implicar el envío de Información personal a Facebook. Las presentes Condiciones del tratamiento de datos se aplican en la medida en que se estipule que debemos tratar Información personal en calidad de Procesador en las condiciones de productos aplicables ("Condiciones de productos aplicables", y cualesquiera productos de Facebook a los que estas afecten, "Productos aplicables"), como las Condiciones de las herramientas para empresas de Facebook y las Condiciones de las audiencias personalizadas a partir de una lista de clientes*
> *[…]*
> *I0. Aceptas que Facebook pueda subcontratar las obligaciones que tiene conforme a las presentes Condiciones del tratamiento de datos a un subprocesador que pueda tener su sede en los Estados Unidos, la Unión Europea (UE), el Espacio Económico Europeo (EEE) u otros países, siempre que sea mediante un acuerdo escrito con dicho subprocesador en el que se le impongan obligaciones que sean como mínimo igual de estrictas que las que se imponen a Facebook en las presentes Condiciones del tratamiento de datos. Si el subprocesador no cumpliese estas obligaciones, Facebook asumirá ante ti plena responsabilidad por el ejercicio de las obligaciones del subprocesador.*
> *[…]*
> *12. En la medida en que el RGPD se aplique al Tratamiento que hagas como Controlador según estas Condiciones del tratamiento de datos, el Apéndice sobre transferencia de datos, que forma parte de dichas Condiciones y queda incorporado a estas por la presente referencia, será de aplicación a las transferencias de Información personal que se originen en Reino Unido, la UE, el EEE o Suiza.”*

DÉCIMO CUARTO: El 15 de abril de 2021, según consta en la diligencia de 16 de abril de 2021, sin estar logado en Facebook y tras visitar la página ***URL.1, aceptando sus cookies, constaban peticiones http GET y POST enviadas al dominio facebook.com con, entre otra, la siguiente información:

1. El valor de la cookie fbp enviado como parámetro dentro de la url.
2. parámetros sw, sh.
3. campo “accept-language”
4. campo “user-agent”
5. parámetro dl con el valor https://***URL.1

Por realizar la operación de login en la cuenta de Facebook en facebook.com usando un usuario de prueba, se instalaban en el navegador cookies, entre otras, c_user, fr.

DÉCIMO QUINTO: El 15 de abril de 2021, según consta en la diligencia de 16 de abril de 2021, estando logado en Facebook con un usuario de prueba y tras visitar la página

***URL.1, constaban peticiones http GET y POST enviadas al dominio facebook.com con, entre otra, la siguiente información:

1. cookies c_user y fr entre otras. El valor de la cookie fbp enviado como parámetro dentro de la url.
2. parámetros sw, sh.
3. campo “accept-language”
4. campo “user-agent”
5. parámetro dl con el valor https://***URL.1

DÉCIMO SÉPTIMO: Del 11 de abril a 10 de mayo de 2021, según se explica en el escrito de la parte reclamada de respuesta de requerimiento de 17 de mayo de 2021, el tráfico dirigido a la web de la parte reclamada desglosado por país de procedencia se repartía de la siguiente forma:

- Para la web ******URL.1*** países de procedencia como ***(…)***.
- Para la web ***URL.1 países de procedencia ***(…).***
- Para ******URL.10*** constaban entre los países de procedencia ***(…).***
- Para ******URL.10*** constaban entre los países de procedencia ***(…).***

DÉCIMO OCTAVO: A 4 de junio de 2021, según se explica en su escrito de respuesta de requerimiento de tal fecha, la parte reclamada estaba localizada al 100% en España y todos sus trabajadores y medios materiales estaban localizados en España.

DÉCIMO NOVENO: A 17 de enero de 2022, según se explica en el escrito de la parte reclamada de 17 de enero de 2022, en la “ventana modal” de “Facebook Login” donde el usuario debía introducir usuario y contraseña, constaba “*Si continúas, Freepik Company tendrá acceso continuo a la información que compartes y Facebook registrará cuando Freepik Company acceda a ella. Más información sobre estos datos que compartes y tu configuración. Política de Privacidad y Condiciones de Freepik Company*.” donde las palabras “*Más información*”, “*Política de privacidad”* y “*Condiciones”* son hiperenlaces.

VIGÉSIMO: Según manifiesta la parte reclamada en su escrito de 17 de enero de 2022, a tal fecha en su política de privacidad decía lo siguiente:

"Puedes abrir tu cuenta como Usuario registrado en Freepik con tu propia cuenta en otras plataformas, como por ejemplo Facebook, utilizando los Logins federados que encontrarás en la parte superior de nuestras webs, y acceder siempre que quieras a través de los mismos, sin necesidad de crear y recordar un nombre de usuario y contraseña específicas para acceder a Freepik.
Esta opción es posible gracias a la colaboración entre Freepik y estas plataformas como corresponsables conjuntos del tratamiento de tus datos personales, para que (i) puedas identificarte directamente en dichas plataformas, (ii) estas nos confirmen que eres quien dices ser, y (iii) nosotros te facilitemos tu ingreso como usuario registrado en Freepik.
Freepik obtiene de estas plataformas, bajo tu consentimiento, tu nombre de usuario, imagen y tu dirección de correo electrónico con la finalidad de proceder a tu registro como usuario de Freepik. Estas plataformas captan identificadores online (dirección IP), identificadores técnicos (de tu dispositivo, así como sus identificadores

publicitarios como "google id" o "apple id") y registran, cada vez que utilizas su login, la fecha y hora de tu acceso a Freepik.
Puedes ejercer tus derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y revocación del consentimiento relacionados con los datos personales obtenidos de estas plataformas (y otros que hayas podido facilitar a Freepik en tu relación con nosotros) dirigiéndote a Freepik en la dirección de correo electrónico suministrada en esta misma política.
¡Ojo! La rectificación o supresión de tus datos en tu cuenta de Freepik, no implica automáticamente la rectificación o supresión de tus datos y cuentas de las plataformas que autentiquen tu identidad: deberás dirigirte también a ellas para ejercer tus derechos.
Para ejercer tus derechos en materia de protección de datos personales en relación con cualesquiera otros datos derivados de tu relación con estas plataformas deberás dirigirte a la plataforma correspondiente.
Puedes obtener información adicional en los siguientes enlaces:
1. Facebook:
Apéndice para responsables y corresponsables de tratamiento de Facebook (disponible en este enlace).
Política de privacidad de Facebook en este enlace. (...)"

VIGÉSIMO PRIMERO: El contrato celebrado entre la parte reclamada y FIL o FACEBOOK INC., de conformidad con el art. 28.3 RGPD, era el que se encontraba en la dirección ***URL.6, según manifiesta la parte reclamada en su escrito de 17 de enero de 2022.

VIGÉSIMO SEGUNDO: A 17 de enero de 2022, según manifiesta la parte reclamada en su escrito de tal fecha, de acuerdo con el “Apéndice sobre transferencia de datos de ciudadanos europeos de Facebook” aplicable desde el 27 de septiembre de 2021 la transferencia de datos a Estados Unidos se basaba en:

a. Cláusulas contractuales tipo (2010) entre responsable (Facebook Ireland) y encargado (Facebook Inc). (Cláusula 6.c) del apéndice).
b. Cláusulas contractuales tipo (2021 P2P o entre encargados de tratamiento) entre las filiales del grupo Facebook. (Cláusula 6.i) del apéndice).

VIGÉSIMO TERCERO: El 08 de febrero de 2022 estando logado en Facebook con un usuario de prueba, y tras visitar la página ***URL.1 aceptando todas sus cookies, no constaban peticiones http enviadas al dominio facebook.com ni facebook.net, según consta en la diligencia de 22 de marzo de 2022.

VIGÉSIMO CUARTO: El 26 de mayo de 2022, según consta en la diligencia de tal fecha:

1. Las cookies cargadas en el navegador al realizar un login en Facebook con un usuario de prueba eran: presence, xs, c_user, fr, sb, datr todas instaladas por el dominio facebook.com.

2. Estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, no constaban peticiones http enviadas a ningún dominio con la palabra “facebook”.

VIGÉSIMO QUINTO: El 14 de septiembre de 2022, según consta en la diligencia de tal fecha, estando previamente logado en una cuenta de Facebook, al visitar la web ***URL.1 y hacer clic en el icono de Facebook para poder registrarse como usuario, se transmitían al domino facebook.com los siguientes datos, entre otros, dentro de una petición http POST:

1. cookies datr, sb, c_user, fr, xs, presence.
2. parámetro “accept-language”.
3. parámetro “user-agent:”
4. dentro del campo referer, la siguiente información:
   “[…]”

VIGÉSIMO SEXTO: A 5 de mayo de 2021, según consta en la diligencia de 15 de septiembre de 2022, FIL manifestó a la DPC que ***(…).***

Siendo su traducción no oficial al castellano:

(…).

También manifestó:

[…]

Siendo su traducción no oficial al castellano:

“[…]

Y que el 10 de septiembre de 2021 FIL manifestó a la Autoridad Irlandesa de Protección de Datos (DPC):

(…).

Siendo su traducción no oficial al castellano:

(…).

De su traducción no oficial del original en inglés a continuación:
(…).
VIGÉSIMO SÉPTIMO: El 20 de julio de 2023 FACEBOOK mantenía publicado en internet las solicitudes FISA que recibe, según consta en la diligencia de tal fecha.

VIGÉSIMO OCTAVO: El 9 de febrero de 2024 la parte reclamada ha decidido eliminado el inicio de sesión o “login federado” de Facebook como alternativa de acceso a los usuarios registrados del código de las distintas webs de su titularidad, según ha explicado en su escrito de 21 de febrero de 2024.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con y según lo establecido en los artículos 47, 48.1 y 64.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

Considerando las circunstancias enumeradas en el artículo 83.2 RGPD, el presente procedimiento de apercibimiento se sigue de conformidad con lo establecido en el artículo 64.3 de la LOPDGDD.

II

Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que la parte reclamada realiza la recogida y tratamiento (a través del servicio de Facebook) de, entre otros, los siguientes datos personales de personas físicas: identificadores únicos de usuarios, la dirección IP, así como otros datos asociados al navegador y a la propia navegación, entre otros tratamientos.

La parte reclamada realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

Por su parte, el artículo 44 del RGPD regula la transferencia de datos personales a terceros países.

III

Alegaciones aducidas

En relación con las alegaciones aducidas, se procede a dar respuesta a las mismas según el orden expuesto por la parte reclamada:

Primera.- Reiteración de manifestaciones

La parte reclamada se mantiene y se remite a las manifestaciones que ha efectuado durante la fase de actuaciones previas de investigación.

a) La normativa estadounidense aplicable no menoscaba el nivel de protección reconocido al interesado por el RGPD

La parte reclamada alega que la Executive Order 12333 y Presidential Policy Directive 28 regulan y limitan la capacidad de acción de inteligencia de las agencias del Gobierno de EEUU fuera de EEUU. Se insiste en que no existe obligación de colaborar con el Gobierno y que la EO 12333 no prevé ningún mecanismo para obligar a las empresas estadounidenses importadoras a colaborar con el Gobierno. Por tanto, con base en la EO 12333, los proveedores de FREEPIK en EEUU no tienen obligación de colaborar con las agencias de inteligencia para aportar datos personales de usuarios europeos.

En cuanto a la Foreign Intelligence Surveillance Act (FISA), la parte reclamada alega que tiene un ámbito objetivo muy específico.

En primer lugar, las comunicaciones, contenidos, metadatos susceptibles de ser interceptados son únicamente aquellos relacionados materialmente con actividades ligadas a terrorismo, actos hostiles, armas de destrucción masiva, actividades clandestinas de espionaje, o con la defensa nacional, o actividades de asuntos exteriores de los EEUU.

En segundo lugar, el requerimiento de información vía sección 702 debe incluir algún tipo de identificador o "selector", como una dirección de email, no puede ser indiscriminada.

En tercer lugar, también es necesario justificar el requerimiento en indicios concretos relacionados con la persona investigada y la información que se espera conseguir. Una Agencia de inteligencia estadounidense está obligada a aportar indicios objetivos y concretos, basados en hechos, para acreditar la probabilidad de que la persona objetivo tenga posesión, acceso o posibilidad de comunicar información relacionada con inteligencia extranjera a potencias extranjeras o a territorios extranjeros. Además, las agencias de inteligencia también deben realizar una evaluación igualmente concreta y justificada en hechos sobre la naturaleza de la información que se espera obtener con el acceso requerido.

En cuarto lugar, se explica que la sentencia Schrems ll alude a la versión de FISA en el momento en el que la Decisión de adecuación sobre el Privacy Shield se emitió, allá por 2016, y no se pronuncia sobre modificaciones posteriores. Una de las más relevantes es que ha restringido la capacidad de requerir, con base en la Sección 702, información basada en palabras clave a encontrar en el contenido de las comunicaciones (lo que se aludía con requerimientos sobre "about") de modo que sólo se puede requerir información basada en identificadores ("selector") de la persona que emite o recibe la comunicación (lo que se alude como requerimientos "from" y/o "to").

Al respecto, alega la parte reclamada que, en un análisis general, ni los datos personales objeto de tratamiento por su parte, ni las categorías de interesados, ni las finalidades de tratamiento incluyen elementos que puedan ser considerados sensibles o de categoría especial. Y nada de ello se encuentra remotamente vinculado al ámbito de aplicación objetivo y subjetivo de la normativa de referencia.

Entiende que las condiciones exigidas en la citada normativa limitan en gran medida el alcance de la vigilancia (en especial, el requisito —como condición previa- de que las agencias de inteligencia estén obligadas a justificar, con base en hechos, que no sólo los targets sino también la información que se pretende conseguir con el requerimiento de acceso, son subsumibles en el ámbito objetivo de dicha normativa).

Y que se pueden identificar situaciones en las que sea la propia organización exportadora la que represente un elemento de interés para las Agencias de Inteligencia, por su naturaleza, integrantes, o sobre todo, por su actividad.

Se alega que la parte reclamada no se integra en la Administración Pública ni presta servicios para ésta. Tampoco está sujeto a ninguna normativa relacionada con la imposición de medidas de protección por razón de su actividad (como actividades estratégicas para la seguridad nacional, actividades de interés general, actividades esenciales o especialmente relevantes, gestión o mantenimiento de infraestructuras críticas o estratégicas, etc.).

Por tanto, entiende que la citada normativa no es aplicable a los datos personales exportados por la parte reclamada. Y que los datos personales objeto de transferencia internacional a los Estados Unidos de Norteamérica están objetivamente fuera del alcance de las Agencias de Inteligencia de este país.

Concluye que las transferencias internacionales de datos personales de la parte reclamada a los Estados Unidos de Norteamérica vinculadas con la Herramienta objeto de requerimiento por la AEPD, no menoscababan el nivel de protección garantizado por el RGPD a sus titulares, ni durante la vigencia del Privacy Shield, ni con posterioridad a su anulación, desde que FACEBOOK impuso su modelo de transferencia con base en Cláusulas Contractuales Tipo.

Al respecto, esta Agencia desea señalar que la propia parte reclamada no niega que el Gobierno de Estados Unidos puede tener acceso a los datos personales de quienes visitan la página web de la parte reclamada, sino que se limita a considerar que teniendo en cuenta la actividad de su página web, las Agencias de Inteligencia no solicitarán información de sus visitantes.

El capítulo V del RGPD prevé diversos instrumentos para garantizar un nivel de protección sustancialmente equivalente al garantizado en la Unión Europea, de conformidad con el artículo 44 del Reglamento, a saber: decisiones de adecuación (artículo 45) y garantías adecuadas (artículo 46). A falta de un nivel de protección equivalente, establece excepciones para situaciones específicas (artículo 49).

Al menos hasta el 10 de julio de 2023 FREEPIK y Meta Platforms, Inc se basaban en la Decisión de adecuación EU-US (“Privacy Shield”) de 2016 para realizar las citadas transferencias internacionales de datos personales.

Respecto a FISA, el TJUE en su sentencia de 16 de julio de 2020, C-311/18, declaró que tal decisión de adecuación no garantizaba un nivel adecuado de protección para las personas físicas debido a la normativa de Estados Unidos pertinente y a la implementación de programas oficiales de vigilancia basados, entre otros, en la

Sección 702 de FISA y E.O.12333 en conjunto con PPD-28 y anuló la citada decisión de adecuación.

Esta Agencia entiende que Meta Platforms, Inc tenía la obligación de proporcionar a las autoridades de Estados Unidos los datos personales de conformidad con el artículo 1881.a del Código de los EE.UU, en caso de que así se le solicitara. Las alegaciones de la parte reclamada no niegan tal obligación, sino que se limitan a considerar que la probabilidad de que tal información fuera solicitada para los visitantes de la web de la parte reclamada era muy improbable.

En cuanto a la adopción de garantías adecuadas, el TJUE ha fallado explícitamente que las transferencias ulteriores a empresas comprendidas en el artículo 50 del EEUU Código "U.S. Code") § 1881a no sólo violan los artículos pertinentes del Capítulo V del RGPD, sino también los artículos 7 y 8 de la CFR, así como la esencia del artículo 47 de la CFR (ver C-362/14 ("Schrems I"), párr. 95.) Por lo tanto, toda transferencia ulterior violaba el derecho fundamental a la privacidad, la protección de los datos y el derecho a la tutela judicial efectiva y a un juez imparcial.

Esta Agencia entiende que Meta Platforms Inc. se califica como un proveedor de servicios electrónicos en el sentido del 50 U.S. Code § 1881(b)(4) y como tal estaba sujeto a la vigilancia de la inteligencia de los Estados Unidos en virtud del 50 U.S. Code § 1881a ("FISA 702"). Como se desprende del propio "Transparency Report" del Facebook (ver https://transparency.facebook.com/government-data-requests/country/US) Facebook está proporcionando activamente datos personales al gobierno de los EEUU bajo el 50 U.S. Code § 1881a.

Como consecuencia, la parte reclamada no podía garantizar una protección adecuada de los datos personales de quienes visitaban su página web (entre otros, de la parte reclamante) que se transferían a Meta Platforms Inc. Por lo tanto, la parte reclamada tenía la obligación legal de abstenerse de transferir los datos de quienes visitaban su página web (entre otros, de la parte reclamante) - o cualquier otro dato personal- a Meta Platforms Inc.

Por último, esta Agencia considera que no se cumplía ningún requisito de los del artículo 49 del RGPD y, en particular, no se había obtenido ningún consentimiento de acuerdo con el artículo 49.1.a).

Por todo lo anteriormente expuesto, esta Agencia entiende que las transferencias internacionales de datos personales de FREEPIK a Meta Platforms Inc, no estaba cubierta por ningún instrumento del artículo 45 y siguientes del RGPD, por lo que se desestima la presente alegación.

b) Inexistencia de culpabilidad

Alega la parte reclamada que no cabe reprocharle jurídicamente culpabilidad o falta de diligencia debida en sus actuaciones.

Y cita:

- Que con fecha 16.07.2020 el TJUE hizo pública la Sentencia invalidó la decisión sobre el "EU-US Privacy Shield" en el fallo C-311/18.

● Que el 11.11.2020 el Comité Europeo de Protección de Datos publicitó dos documentos relevantes para cualquier empresa que estuviera realizando tratamientos de datos: a) las directrices sobre medidas adicionales aplicables para legitimar las transferencias internacionales, y b) el documento relativo a las “garantías esenciales europeas”. En dichos documentos no se indica, sin más, ni mucho menos, que toda transferencia internacional a EEUU sería ilegal, posibilitando realizar las mismas en condiciones que FREEPIK cumple.
● Que el 11.11.2020 , casi con inmediatez al planteamiento del Comité y de la Comisión aludidos, se comunicó a esta parte la denuncia.
● Que el 14.11.2020 la Comisión Europea publicó sus nuevos modelos provisionales de “cláusulas contractuales tipo”, en los que acoge explícitamente el planteamiento del “risk based approach” para evaluar el riesgo concreto para los interesados, derivado de la concreta transferencia internacional.
● La denuncia se había presentado el 17.08.2020 , cuando ni siquiera se conocía el planteamiento del Comité ni de la Comisión. En ella se alegaba que las transferencias eran ilegales, cuando ni siquiera ello se afirmaba por la STJUE aludida.

Alega también que debe valorarse el grado de cumplimiento en un clima de incertidumbre oficial generalizado, (posterior a la STJUE y a la denuncia). La Audiencia Nacional (Sala de lo Contencioso), en Sentencia de 23.04.2019, dictada en el procedimiento SAN 1801/2019, nº de Recurso 88/2017, ha declarado que el Comité Europeo de Protección de Datos, como organismo de la Unión, con personalidad jurídica, “emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento”, de acuerdo con la literalidad del art. 70.1.e) RGPD , y que, siendo el Comité el órgano encargado de interpretar el alcance de los preceptos el RGPD, en el supuesto de existir importantes y razonables dudas suscitadas al respecto de la aplicación de uno de los preceptos del RGPD, ello no permitiría sustentar la imposición de una sanción.

Al respecto, esta Agencia desea señalar que todas estas cuestiones han sido evaluadas y tenidas en cuenta a la hora de decidir sobre qué poder correctivo de los citados en el artículo 58.2 del RGPD se habría de aplicar en el presente caso y por ello (entre otras razones) se ha optado por seguir un procedimiento de apercibimiento. Pero nada de esto obsta a que las transferencias internacionales llevadas a cabo en el contexto de la actividad que realizaba la parte reclamada no cumplían con los elementos exigidos por el artículo 44 del RGPD y que era obligación de la parte reclamada comprobar que sí lo era y dejar de utilizar los servicios en cuestión si éstos no cumplían lo exigido.

Por lo que se desestima la presente alegación.

c) Actuaciones llevadas a cabo

Desde la publicación del fallo del TJUE, la parte reclamada inició un intenso proceso de revisión de los instrumentos jurídicos en los que basa sus transferencias internacionales de datos a Estados Unidos, entre ellas las derivadas del uso de la Herramienta, llevando a cabo las siguientes actuaciones:

● Comunicación con sus proveedores externos a la UE y envío de cuestionarios para mapear las transferencias internacionales de datos, y

recopilar información relacionada con las circunstancias subrayadas por la sentencia Schrems II.
● Comunicaciones con Facebook requiriendo documentación y colaboración.
● Contacto con la asociación denunciante NOYB, poniéndose a su disposición para entablar un diálogo, informar de los posibles perjuicios causados y explicar su posición. No se ha recibido respuesta de NOYB.
● Estudio, por parte del DPD de la Compañía, de la normativa estadounidense destacada por la sentencia Schrems II, y revisión de las transferencias internacionales realizadas por la parte reclamada a la luz de la misma.
● Solicitud de una Opinión Jurídica (Legal Opinion) a DLA Piper, despacho estadounidense de reconocido prestigio, especializado en dicha normativa sobre las conclusiones preliminares del DPD, y en general sobre la aplicación de la normativa estadounidense en lid y sus implicaciones concretas sobre la parte reclamada.

Al respecto, esta Agencia desea señalar que valora positivamente que la parte reclamada revisara los instrumentos sobre los que basaba sus transferencias internacionales a Estados Unidos y que todo ello ha sido tenido en cuenta a la hora de decidir sobre qué poder correctivo de los citados en el artículo 58.2 del RGPD se habría de aplicar en el presente caso y por ello (entre otras razones) se ha optado por seguir un procedimiento de apercibimiento. Pero nada de esto obsta a que las transferencias internacionales llevadas a cabo en el contexto de la actividad que realizaba la parte reclamada no cumplían con los elementos exigidos por el artículo 44 del RGPD y que era obligación de la parte reclamada comprobar que sí lo era y dejar de utilizar los servicios en cuestión si éstos no cumplían lo exigido.

Por lo que se desestima la presente alegación.

d) Actuación de la parte reclamante

Alega la parte reclamante que concurren circunstancias especiales en la parte reclamante que permiten poner en duda la buena fe procesal que debe regir su solicitud, y que deslegitiman sus pretensiones. Entiende que se podría estar utilizando la normativa de protección de datos como subterfugio formalista para dirigir ataques instrumentalizados y constantes frente a Facebook, convirtiendo en “rehenes” a cientos de empresas que utilizan sus servicios (como la parte reclamada), en un posible interés (del denunciante) que nada tiene que ver con la protección de sus datos personales en la parte reclamada. Y cita para ello el artículo 7 del Código Civil y la Sentencia del TS de 20/05/2002.

Alega que su ejercicio se produce de una forma que resulta finalmente abusiva en relación con los fines pretendidos en el ejercicio de los citados derechos, utilizándose de manera anormal con ausencia de una finalidad o un interés serio y legítimo y un exceso en el ejercicio de su derecho”.

Reseña la parte reclamada que:
● Con fecha 14.08.2020 , cuando ni siquiera había transcurrido un mes desde la Sentencia TJUE aludida, el denunciante visitó la web de FREEPIK COMPANY, S.L., a fin de instrumentalizar una denuncia posterior contra FACEBOOK IRELAND, LTD, y

FACEBOOK INC., incluyendo en la misma a la empresa española FREEPIK COMPANY, S.L.

● Con fecha 17.08.2020 , (es decir, tres días más tarde de la visita a la web, y sin haber realizado un solo requerimiento sobre sus datos a FREEPIK COMPANY, S.L.), se interpuso una denuncia directamente en la Agencia Española de Protección de Datos, alegando lo siguiente:

- ● Que había visitado la web de FREEPIK COMPANY, S.L. y que comprobó que la web de FREEPIK COMPANY, S.L. tenía incrustado el código HTML de los servicios de Facebook.
- ● Que habiendo transcurrido más de un mes desde la Sentencia del TJUE, FREEPIK COMPANY, S.L. sigue realizando transferencias internacionales (sic) “sin garantizar una protección adecuada de los datos personales de la reclamante”, que, según NOYB, podría ser “uno de los miles de usuarios”
- ● Que “ la transferencia de los datos de la reclamante a los Estados Unidos es ilegal ”.

● En la misma fecha en la que se interpuso la denuncia (17.08.2020), NOYB hizo público un comunicado publicitario en su propia web, anunciando que había interpuesto 101 denuncias frente a 101 empresas.

El texto de NOYB daba un listado de los denunciados, solicitaba financiación , y cargaba principalmente contra Facebook, a la vez que se ponía a disposición de las empresas (como FREEPIK COMPANY, S.L.) facilidades para cumplir con la normativa.

Al respecto, esta Agencia desea señalar que no es objeto del presente procedimiento la actuación de NOYB ni de la parte reclamante. Simplemente se trata de determinar si la parte reclamada cumplía con los requisitos del artículo 44 del RGPD. Por lo que se desestima la presente alegación.

e) Rol de FACEBOOK

La parte reclamada indica que los Términos y condiciones que FACEBOOK ofrece a sus clientes en régimen de “adhesión” describen a FACEBOOK con dos roles, en lo que aquí interesa:

a) Un grupo de tratamientos en los que FACEBOOK, interpretando de forma estricta la sentencia “Fashion Id”, reconoce su rol como corresponsable, describe a FACEBOOK Inc. como encargado de tratamiento y al cliente (la parte reclamada) como corresponsable.

b) Un segundo grupo de tratamientos, en el que se califica al cliente (la parte reclamada) como Responsable de tratamiento, que “indica” a FACEBOOK que haga tal o cual cosa en su nombre como encargado de tratamiento. Califica igualmente a FACEBOOK Inc. como “Subencargado de tratamiento” para el “almacenamiento y tratamiento más extenso de datos”. (Apéndice sobre transferencia de datos de la UE ***URL.5).

La parte reclamada discrepa de esta configuración jurídica y llama la atención sobre las “Guidelines on targeting of social media users” del EDPB, publicadas en septiembre de 2020, y por tanto de fecha posterior a la versión de las “Condiciones de Tratamiento Actualizadas” de FACEBOOK de fecha 31.08.2020.

De acuerdo con la interpretación de la parte reclamada, basada en la literalidad del apartado 5.2.1, págs. 13 y 14 de las referidas “guidelines”, los tratamientos en los que FACEBOOK IRELAND y FREEPIK son corresponsables alcanzarían, no sólo a lo regulado en los apartados 2.a.iii y 2.a.v.i. como pretende FACEBOOK (tratamientos en los que está comprendido el del Facebook login o inicio de sesión de FACEBOOK), sino también a los incluidos en los apartados 2.a.ii.1 y 2.a.ii.2.

Explica la parte reclamada que FACEBOOK distingue, en su propia documentación y nomenclatura, entre “datos de información de contacto” y “datos de eventos”.

a. Los datos de información de contacto que son, básicamente, identificadores.
b. Los datos de “eventos” que son “información adicional sobre personas y sus acciones en las páginas web (las de la parte reclamada)” (visitas, compras de productos, u otras que determine el cliente, la parte reclamada no generaba ninguna nueva aparte de las predeterminadas por FACEBOOK).

De acuerdo con este mismo documento, FACEBOOK (estipulación 5.a.i) se autoconfiguraba como Encargado de tratamiento (y por tanto la parte reclamada era Responsable de tratamiento) en relación con sus estipulaciones siguientes:

> 2.a.i.1. La “información de contacto” para la búsqueda de coincidencias. Por ejemplo: la parte reclamada podía entregar a FACEBOOK el listado de direcciones de correo electrónico de sus “usuarios premium” para que FACEBOOK no les impactara en el contexto de sus campañas publicitarias. FACEBOOK manifestó utilizar un sistema de cifrado de estas direcciones que conseguía cruzar ambas bases de datos (la de FACEBOOK y la de la parte reclamada) sin llegar a “leer” datos personales nuevos, distintos de los que sean objeto ya de tratamiento por su parte, y después los suprime.
>
> 2.a.ii.1 y 2: “datos de eventos” para servicios de medición y análisis (preconfigurados ya por FACEBOOK o creados y personalizados por el cliente): informe sobre el rendimiento de las campañas estadísticas sobre personas y uso de una página web.

A juicio de la parte reclamada, es evidente que ella no “indicaba nada” a FACEBOOK , quien tenía ya prefigurado y disponible aquello que la parte reclamada podía o no hacer.

Por otro lado, alega la parte reclamada que el hecho de que un encargado de tratamiento únicamente concediera una “licencia no exclusiva e intransferible” sobre el resultado del servicio con acceso a datos ordenado o “indicado” por la parte reclamada a FACEBOOK, se compadece mal, por decir lo menos, con la teórica posición de ambos como Encargado y responsable de tratamiento.

Interpreta la parte reclamada -con base en la literalidad del apartado 5.2.1, pgs 13 y 14 de las mencionadas Guidelines on targeting of social media users del EDPB-, que ella era corresponsable junto con FACEBOOK en relación con los tratamientos de datos producidos como directa consecuencia de la selección por parte de la parte reclamada de los criterios de targeting ofrecidos por FACEBOOK, y los subsiguientes impactos publicitarios sobre los usuarios de dicha plataforma. Y también sobre el reporte por

parte de FACEBOOK de datos agregados a la parte reclamada en relación con el resultado y rendimiento de cada campaña publicitaria.

Respecto a FACEBOOK como Corresponsable de tratamiento junto con la parte reclamada, de acuerdo con este mismo documento, indica la parte reclamada que FACEBOOK se autoconfiguraba (estipulación 5.a.ii) como corresponsable de tratamiento, junto con FREEPIK, en relación con:

> 2.a.iii.1 : Cesión de “datos de eventos” para dirigir campañas publicitarias a personas que interactúen con FREEPIK (“Retargeting”).
>
> 2.a.v.1.: Cesión de “datos de eventos” para mejorar la segmentación de anuncios y optimización de entregas de campañas publicitarias, correlación entre esos datos de eventos y las personas que usan productos de FACEBOOK , mejorar la eficacia de los modelos de entrada anuncios, determinar la relevancia de los anuncios para las personas.

Alega la parte reclamada que ella no indicaba a FACEBOOK que captara ningún dato: la plataforma los captaba en cualquier caso: simplemente FACEBOOK ofrecía la explotación publicitaria de “audiencias” con base en toda esa información personal de sus usuarios, debidamente clasificada y perfilada.

Al respecto, esta Agencia desea señalar que la parte reclamada, como titular de la página web, adoptó la decisión de implementar las Herramientas de Facebook Business en su sitio web ***URL.1. En particular, insertó un código JavaScript, proporcionado por Meta Platforms, Inc, en el código fuente de su página web, por lo que este código JavaScript fue ejecutado en el navegador de quienes visitan la página web (entre otros, la parte reclamante) durante su visita a la misma.

Como resultado, la parte reclamada decidió sobre las finalidades y medios del tratamiento de datos relacionados con la herramienta, por lo que debe ser considerada responsable de tratamiento de acuerdo con el artículo 4.7 del RGPD.

En cuanto al rol de Meta Platforms, Inc, a pesar de las extensas actuaciones de investigación, esta Agencia no ha encontrado evidencias suficientes para calificar a Meta Platforms, Inc como responsable del tratamiento. Por lo que se desestima la presente alegación.

Segunda.- Implementación de mecanismos más adecuados en cada momento

Alega la parte reclamada que ha implementado los mecanismos jurídicos de transferencia y medidas más adecuados entre los disponibles en cada momento para proteger adecuadamente los datos personales de sus usuarios.

Y se remite a sus escritos presentados durante las actuaciones previas de investigación, en los que se comunicaron la implementación y uso de las SCCs entonces -2020- vigentes, del nuevo set de SCCs aprobado por la Comisión Europea en 2021, la desactivación del Facebook pixel en mayo de 2021 y el recientemente aprobado marco DPF.

Al respecto, esta Agencia se reitera en que el capítulo V del RGPD prevé diversos instrumentos para garantizar un nivel de protección sustancialmente equivalente al garantizado en la Unión Europea, de conformidad con el artículo 44 del Reglamento, a saber: decisiones de adecuación (artículo 45) y garantías adecuadas (artículo 46). Y a falta de un nivel de protección equivalente, establece excepciones para situaciones específicas (artículo 49).

Al menos hasta el 10 de julio de 2023 la parte reclamada y Meta Platforms, Inc se basaban en la Decisión de adecuación EU-US ("Privacy Shield") de 2016 para realizar las citadas transferencias internacionales de datos personales.

Sin embargo, el TJUE en su sentencia de 16 de julio de 2020, C-311/18, declaró que tal decisión de adecuación no garantizaba un nivel adecuado de protección para las personas físicas debido a la normativa de Estados Unidos pertinente y a la implementación de programas oficiales de vigilancia basados, entre otros, en la Sección 702 de FISA y E.O.12333 en conjunto con PPD-28 y anuló la citada decisión de adecuación.

Esta Agencia entiende que Meta Platforms, Inc tenía la obligación de proporcionar a las autoridades de Estados Unidos los datos personales de conformidad con el artículo 1881.a del Código de los EE.UU.

Por su parte, la parte reclamada tampoco podía basar la transferencia de datos en las cláusulas contractuales tipo de protección de datos previstas en Artículo 46(2)(c) y (d) del RGPD si el tercer país de destino no garantizaba una protección adecuada, con arreglo a la legislación de la UE, de los datos personales transferidos con arreglo a esas cláusulas (ver los párr. 134 y 135 de la Sentencia). El TJUE ha fallado explícitamente que las transferencias ulteriores a empresas comprendidas en el artículo 50 del EEUU Código "U.S. Code") § 1881a no sólo violan los artículos pertinentes del Capítulo V del RGPD, sino también los artículos 7 y 8 de la CFR, así como la esencia del artículo 47 de la CFR (ver C-362/14 ("Schrems I"), párr. 95.) Por lo tanto, toda transferencia ulterior viola el derecho fundamental a la privacidad, la protección de los datos y el derecho a la tutela judicial efectiva y a un juez imparcial.

Meta Platforms Inc. se califica como un proveedor de servicios electrónicos en el sentido del 50 U.S. Code § 1881(b)(4) y como tal está sujeto a la vigilancia de la inteligencia de los Estados Unidos en virtud del 50 U.S. Code § 1881a ("FISA 702"). Como se desprende del propio "Transparency Report" de Facebook (ver https://transparency.facebook.com/government-data-requests/country/US) Facebook está proporcionando activamente datos personales al gobierno de los EEUU bajo el 50 U.S. Code § 1881a.

Como consecuencia, la parte reclamada no podía garantizar una protección adecuada de los datos personales de quienes visitaban su página web (entre otros, de la parte reclamante) que se transferían a Meta Platforms Inc. Por lo tanto, la parte reclamada tenía la obligación legal de abstenerse de transferir los datos de quienes visitaban su página web (entre otros, de la parte reclamante) - o cualquier otro dato personal- a Meta Platforms Inc.

Por último, esta Agencia considera que tampoco no se cumple ningún requisito de los del artículo 49 del RGPD y, en particular, no se ha obtenido ningún consentimiento de acuerdo con el artículo 49.1.a).

Por lo demás, esta Agencia desea señalar que, aun en el supuesto de que se hubieran aprobado nuevos instrumentos normativos que hicieran que no existiera infracción por parte de la parte reclamada a partir de su aprobación, ello no obsta a que se hubiera comprobado que la parte reclamada anteriormente había infringido lo dispuesto por el artículo 44 del RGPD.

Por todo lo expuesto, se desestima la presente alegación.

Tercera.- No existencia de infracción

Alega la parte reclamada que, desde la aprobación en los EEUU de Norteamérica y en la Unión Europea de los instrumentos normativos a los que se referirá a continuación, y de su aplicación a Meta Platforms Ireland Limited (antigua Facebook Ireland) y Meta Platforms Inc (antigua Facebook Platforms Inc), no existe infracción ni necesidad de imponerse por la Agencia ulteriores medidas de regularización.

Al respecto, esta Agencia desea señalar que, aun en el supuesto de que se hubieran aprobado nuevos instrumentos normativos que hicieran que no existiera infracción por parte de la parte reclamada a partir de su aprobación, ello no obsta a que se hubiera comprobado que la parte reclamada anteriormente había infringido lo dispuesto por el artículo 44 del RGPD. Por lo que se desestima la presente alegación.

Cuarta: Entrada en vigor de nueva normativa relevante a ambos lados del Atlántico con la aprobación del “Trans-Atlantic Data Privacy Framework”

4.1.- Octubre de 2022

Alega la parte reclamada que, desde la parte estadounidense, y como condición indispensable para la aprobación e implementación del “Trans-Atlantic Data Privacy Framework” (o “DPF” en inglés) en Octubre se publicó en los EEUU de Norteamérica la Executive Order Presidencial 14.086 On Enhancing Safeguards For United States Signals Intelligence Activities en cuya virtud se establecen:

● Un Sistema de revisión de denuncias en dos instancias:

> Explica la parte reclamada que, en primera instancia, los interesados de “estados cualificados” (entre los que se encontrarán los estados miembros de la UE) pueden interponer denuncia ante sus propias autoridades públicas.
>
> Y que dicha denuncia se remite al CLPO (Civil Liberties Protection Officer) que valora si se ha cometido una “infracción cubierta” (una infracción derivada de actividades de “signal intelligence activities”) de la constitución USA, FISA, la EO 12.333, esta nueva EO o cualquier norma nueva que se implemente al efecto.

Y que si el CLPO determina la existencia de una infracción cubierta, identifica la solución adecuada a la misma, comunicándosela al Assistant Attorney General for National Security.

Después de su revisión, el CLPO confirma por escrito al denunciante si (a) no se ha identificado una infracción cubierta o que (b) el CLPO ha dictaminado una determinación requiriendo su solución adecuada.

Indica la parte reclamada que, en segunda instancia, el denunciante puede solicitar la revisión de la resolución del CLPO ante un tribunal administrativo de nuevo cuño, el DPRC (Data Protection Review Court).

En este tribunal se designa una sala de tres miembros y un Special Advocate, que revisan el expediente elaborado por el CLPO, junto con los antecedentes aportados por el denunciante, el Special Advocate o las autoridades de vigilancia.

También pueden ordenar la realización de diligencias adicionales al CLPO. Si el Tribunal concluye la existencia de una infracción cubierta, puede ordenar su solución adecuada, que es vinculante para las autoridades de vigilancia.

Al final del procedimiento, el tribunal confirma por escrito al denunciante si (a) no se ha identificado una infracción cubierta o que (b) el tribunal ha dictaminado una determinación requiriendo su solución adecuada.

● Un nuevo sistema de salvaguardias centradas en los principios de limitación de la finalidad y proporcionalidad.

En cuanto a la proporcionalidad, explica la parte reclamada que la EO 14086 limita las actividades de inteligencia de “señales” de Estados Unidos de forma vinculante para las Agencias de Inteligencia.

Con este fin, establece una lista de doce "objetivos legítimos" para la recogida y cuatro "objetivos prohibidos".

Y que la captación de datos dentro de EE.UU. (es decir, todos los datos que se transfieren a EE.UU.) debe tener objetivos específicos. La recogida de datos fuera de EE.UU. debe dar prioridad a la recogida selectiva, y la recogida masiva se limita a situaciones en las que un objetivo validado no puede razonablemente obtenerse mediante la recogida selectiva, y sólo en la medida y de una manera que sea proporcional a la finalidad de inteligencia validada.

● Requerimientos concretos para que las autoridades de inteligencia norteamericanas actualicen sus políticas y procedimientos.

Señala la parte reclamada que estos requerimientos de la EO 14086 han sido cumplidos a través de la regulación sobre el Data Protection Review Court publicada por el U.S. Attorney General (el “Reglamento AG”) y por los nuevos “Procedimientos” de las agencias integradas en la “Comunidad de Inteligencia”.

4.2.- Julio de 2023

Alega la parte reclamada que el pasado 10 de julio de 2023 se aprobó definitivamente el acuerdo marco por decisión de adecuación por la Comisión Europea, que entró en vigor el mismo 10 de julio de 2023 como fecha de publicación, y bajo la denominación ya mencionada de “EU-US Data Privacy Framework” o “DPF”.

Y que la adopción comunitaria de la Decisión de Adecuación de 10 de julio de 2023 hizo efectiva la designación por el Fiscal General de la UE y los tres Estados miembros del EEE/AELC como ‘Estados cualificados’ a efectos de la aplicación del mecanismo de recurso.

Añade que se estableció un sistema equivalente al preexistente en el Privacy Shield al que se añadieron las nuevas garantías expuestas en el punto anterior.

Explica la parte reclamada que a partir de dicha fecha:

● La transferencia de datos personales a Estados Unidos, sea a proveedores de servicios estadounidenses o a una filial de su Grupo de sociedades, se entiende automáticamente validada por la decisión de adecuación ratificada si se encuentran certificados en este nuevo marco DPF;

● Alternativamente, todas las entidades que estuvieran certificadas válidamente en el sistema anterior (Privacy Shield), se consideran provisionalmente certificados durante un plazo máximo de 3 meses desde la entrada en vigor (hasta 10 de octubre de 2023), al término del cual deberán haber actualizado sus políticas de privacidad, sin necesidad de pasar por un nuevo proceso de certificación;

● La Comisión Europea, en su decisión de adecuación y concretamente en su Considerando 7 declara que “ha analizado detenidamente la legislación y la práctica estadounidenses, incluidos la Executive Order 14.086 y el Reglamento AG. Sobre la base de las constataciones expuestas en los considerandos 9 a 200 de la decisión de adecuación, la Comisión concluye que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos en virtud del DPF por un responsable o un encargado del tratamiento radicado en la Unión Europea a organizaciones certificadas en el marco en los Estados Unidos”.

En opinión de la parte reclamada, la rotundidad de la Comisión Europea en la citada decisión de adecuación, en la que analiza el ordenamiento jurídico estadounidense a la luz de los principios y garantías esenciales europeas deja lugar a pocas dudas sobre la licitud de las transferencias internacionales realizadas entre empresas y organizaciones de la UE y las ubicadas en los Estados Unidos de Norteamérica.

Al respecto, esta Agencia desea señalar que los hechos reclamados que dieron origen al presente procedimiento ocurrieron el 14 de agosto de 2020.

El 22 de enero de 2021 esta Agencia pudo comprobar que estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, dicha visita consta en la sección “Actividad fuera de Facebook” asociada al usuario logado.

El 15 de abril de 2021 esta Agencia comprobó que sin estar logado en Facebook y tras visitar la página ***URL.1, aceptando sus cookies, constan peticiones http GET y POST enviadas al dominio facebook.com con, entre otra, la siguiente información:

1. El valor de la cookie fbp enviado como parámetro dentro de la url.
2. parámetros sw, sh.
3. campo “accept-language”
4. campo “user-agent”
5. parámetro dl con el valor ***URL.1

Y que exclusivamente por realizar la operación de login en la cuenta de Facebook en facebook.com usando un usuario de prueba, se instalan en el navegador cookies, entre otras, c_user, fr.

También con fecha 15 de abril de 2021 se comprueba que estando logado en Facebook con un usuario de prueba y tras visitar la página ***URL.1, constan peticiones http GET y POST enviadas al dominio facebook.com con, entre otra, la siguiente información:

1. cookies c_user y fr entre otras. El valor de la cookie fbp enviado como parámetro dentro de la url.
2. parámetros sw, sh.
3. campo “accept-language”
4. campo “user-agent”
5. parámetro dl con el valor https://***URL.1

Con fecha 21 y 22 de enero 2021 el contenido de la url ***URL.5 era el siguiente:

“Apéndice sobre transferencia de datos de la UE de Facebook

Este Apéndice sobre transferencia de datos de la UE ("Apéndice transferencia de datos") se aplica en la medida en que FIL actúe como Procesador de Datos de la UE de conformidad con las condiciones del producto aplicables, como las Condiciones de las herramientas para empresas de Facebook o las Condiciones de las audiencias personalizadas a partir de una lista de clientes ("Condiciones del producto aplicables"), y las transferencias de los Datos de la UE que se originen en el Reino Unido, la UE, el EEE o Suiza se realicen a su subprocesador Facebook, Inc.

1. Teniendo en cuenta las circunstancias, indicas a FIL que transfiera los Datos de la UE a Facebook, Inc. en los Estados Unidos para su almacenamiento y un Tratamiento más extenso. Las Cláusulas se aplican entre tú y Facebook, Inc. en relación con las transferencias de los Datos de la UE que se originen en el Reino Unido, la Unión Europea, el Espacio Económico Europeo o Suiza a Facebook, Inc., a menos que en el RGPD se permitan de otro modo.

a. Respecto a las Cláusulas, tú eres el "exportador de datos" y Facebook, Inc. es el "importador de datos", de acuerdo con la definición de estos términos en dichas Cláusulas.

[…]

8. En este Apéndice sobre transferencia de datos:

a. "Cláusulas" hace referencia a las cláusulas tipo de protección de datos para la transferencia de datos personales a los procesadores establecidos en terceros países que no garanticen un nivel de protección de los datos adecuado, según se describe en el artículo 46 del RGPD y de acuerdo con la

aprobación de la Decisión 2010/87/CE de la Comisión Europea del 5 de febrero de 2010 (pero sin incluir las cláusulas ilustrativas opcionales).
[…]"

Por su parte, con fecha 21 y 22 de enero 2021 el contenido de la url ***URL.6 era el siguiente:

"Condiciones del tratamiento de datos
Aceptas que el uso que hagas de determinados Productos de Facebook puede implicar el envío de Información personal a Facebook. Las presentes Condiciones del tratamiento de datos se aplican en la medida en que se estipule que debemos tratar Información personal en calidad de Procesador en las condiciones de productos aplicables ("Condiciones de productos aplicables", y cualesquiera productos de Facebook a los que estas afecten, "Productos aplicables"), como las Condiciones de las herramientas para empresas de Facebook y las Condiciones de las audiencias personalizadas a partir de una lista de clientes
[…]
I0. Aceptas que Facebook pueda subcontratar las obligaciones que tiene conforme a las presentes Condiciones del tratamiento de datos a un subprocesador que pueda tener su sede en los Estados Unidos, la Unión Europea (UE), el Espacio Económico Europeo (EEE) u otros países, siempre que sea mediante un acuerdo escrito con dicho subprocesador en el que se le impongan obligaciones que sean como mínimo igual de estrictas que las que se imponen a Facebook en las presentes Condiciones del tratamiento de datos. Si el subprocesador no cumpliese estas obligaciones, Facebook asumirá ante ti plena responsabilidad por el ejercicio de las obligaciones del subprocesador.
[…]
12. En la medida en que el RGPD se aplique al Tratamiento que hagas como Controlador según estas Condiciones del tratamiento de datos, el Apéndice sobre transferencia de datos, que forma parte de dichas Condiciones y queda incorporado a estas por la presente referencia, será de aplicación a las transferencias de Información personal que se originen en Reino Unido, la UE, el EEE o Suiza."

Con fecha 10 de septiembre de 2021 FIL remite a la Autoridad Irlandesa de Protección de Datos (DPC), la siguiente información y manifestaciones:

El 26 de mayo de 2022 esta Agencia comprueba que las cookies cargadas en el navegador al realizar un login en Facebook con un usuario de prueba son; presence, xs, c_user, fr, sb, datr todas instaladas por el dominio facebook.com.

El 16 de mayo de 2022 META PLATFORMS INC (antigua FACEBOOK INC.) remite a la Autoridad Austríaca de Protección de Datos (DSB), la siguiente información y manifestaciones, de su traducción no oficial del original en alemán:

(…).

El 14 de septiembre de 2022 se comprueba que estando previamente logado en una cuenta de Facebook, al visitar la web ***URL.1 y hacer clic en el icono de Facebook

para poder registrarse como usuario, se transmiten al domino facebook.com los siguientes datos, entre otros, dentro de una petición http POST:

1. cookies datr, sb, c_user, fr, xs, presence.
2. parámetro “accept-language”.
3. parámetro “user-agent:”
4. dentro del campo referer, la siguiente información:
   […]

El 5 de mayo de 2021 FIL manifestó a la Autoridad Irlandesa de Protección de Datos (DPC) lo siguiente (traducción no oficial, en inglés el original):

(…).

Por tanto, en el presente procedimiento consta que entre agosto de 2020 y septiembre de 2022, la parte reclamada tenía instalado en sus páginas web el servicio de Facebook Login, el cual recababa datos personales de los visitantes, que eran transferidos a FB Inc, en los Estados Unidos.

Los “nuevos instrumentos normativos” a que hace referencia la parte reclamada son de octubre 2022 y julio 2023. Aun en el supuesto de que éstos hicieran que no existiera infracción por parte de la parte reclamada a partir de su aprobación, ello no obsta a que se hubiera comprobado que la parte reclamada anteriormente había infringido lo dispuesto por el artículo 44 del RGPD. Por lo que se desestima la presente alegación.

Quinta. - Aplicación del DPF a Facebook

En cuanto a la relación de Freepik con Meta Platforms Ireland Limited (antigua Facebook Ireland) y Meta Platforms Inc (antigua Facebook Platforms Inc), la parte reclamada reseña la documentación disponible que acredita la aplicación efectiva del DPF a Facebook que incluye los contratos de adhesión aplicables (actualizados de acuerdo con las condiciones del DPF descritas anteriormente):

● La homologación de Meta Platforms Inc. en el DPF.

● Las políticas de privacidad de Facebook, que se han actualizado en septiembre del 2023 conforme a lo establecido anteriormente.

Al respecto, esta Agencia se reitera en lo dicho anteriormente.

Es decir, en el presente procedimiento consta que entre agosto de 2020 y septiembre de 2022, la parte reclamada tenía instalado en sus páginas web el servicio de Facebook Login, el cual recababa datos personales de los visitantes, que eran transferidos a FB Inc, en los Estados Unidos.

Los “nuevos instrumentos normativos” a que hace referencia la parte reclamada son de octubre 2022 y julio 2023. Aun en el supuesto de que éstos hicieran que no existiera infracción por parte de la parte reclamada a partir de su aprobación, ello no obsta a que se hubiera comprobado que la parte reclamada anteriormente había

infringido lo dispuesto por el artículo 44 del RGPD. Por lo que se desestima la presente alegación.

Escrito del 21 de febrero de 2024

En su escrito de 21 de febrero de 2024, la parte reclamada informa a esta Agencia que ha decidido eliminar el inicio de sesión o "login federado" de Facebook como alternativa de acceso a los usuarios registrados del código de las distintas webs de Freepik. Y que esta eliminación se ha hecho efectiva el día 9 de febrero de 2024.

Al respecto, esta Agencia desea señalar que en vista de esta información considera conforme a derecho no ordenar a la parte reclamada la adopción de medidas que contempla el artículo 58.2 d) del RGPD.

IV
Transferencias de datos personales a terceros países

Datos personales

El artículo 4 "Definiciones" del RGPD define a los datos personales de la siguiente manera:

"A efectos del presente Reglamento se entenderá por:

***1)** «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; (…)"*

En el presente caso, la parte reclamada – como titular de la página web- ha implementado las herramientas de Facebook Business en su sitio web ***URL.1. Como resultado de esta implementación al menos la siguiente información del terminal de los visitantes de la página web (entre otra, la de la parte reclamante) ha sido transmitida a los servidores de Meta Platforms, Inc:

- Dirección IP;
- User agent;
- Sistema operativo móvil y navegador;
- Información sobre el servidor host (la página web que cuenta con la funcionalidad login);
- Fecha y hora de la visita a la página web;
- Idioma del contenido (el idioma del público al que se dirige la página web)
- Ubicación (normalmente el código del país a que se refiere el contenido del campo idioma en el encabezado HTTP
- HTTP referrer (URL de la página en que está ubicada la persona)

- Datos del puerto de visualización (la resolución de la pantalla del dispositivo empleado)
- Identificador de usuario
- Fichas de acceso en caché
- Encabezados de solicitud HTTP estándar que aún no se encontraban en la lista
- Valores almacenados en las cookies FB.

Como resultado de la implementación de las Herramientas de Facebook Business en ***URL.1 se instalaron cookies en el dispositivo de los visitantes de la página web (entre otros, en el de la parte reclamante), que contienen un valor único generado de forma aleatoria. Esto hace posible personalizar el dispositivo de quienes visitaron la página web (entre otros, la parte reclamante) y grabar la actividad de navegación de estos visitantes (entre quienes se encontraba la parte reclamante) para poder mostrarle publicidad personalizada adecuada.

En cualquier caso, al menos Meta Ireland tenía la opción de vincular los datos que recibió como resultado de la implementación de Facebook Business Tools en ***URL.1 con la cuenta de Facebook de los visitantes de la página web (entre otros, de la parte reclamante).

Por ejemplo, de los términos de uso de Facebook Business Tools se desprende claramente que Facebook Business Tools se utiliza para intercambiar información con Facebook.

No es necesario que la parte reclamada pueda establecer por sí una identificación personal, es decir, que cuente con toda la información necesaria para su identificación (véanse las sentencias del Tribunal de Justicia de la Unión Europea de 20 de julio de 2008, Diciembre de 2017, C-434/16, apartado 31, y de 19 de octubre de 2016, C-582/14, apartado 43).

Esto se encuentra en línea con la sentencia *Fashion ID*. El TJUE asumió que la inclusión de un botón “Me gusta” en una página web -sin importar si se ha hecho click o no en el botón - desencadena el tratamiento de datos personales (sentencia del 29 de julio de 2018, C-40/17, párrafo 80). Desde el punto de vista del TJUE, no resulta necesario que el titular de una determinada página web pudiera establecer un identificador personal.

Los pronunciamientos del TJUE puede ser aplicados al presente caso, dado que de acuerdo a los Términos de uso, los botones “Me Gusta” y Facebook Login y Facebook Pixel se encuentran entre las Herramientas de Facebook Business.

Por tanto, se trata de datos personales, de acuerdo con el artículo 4.1 del RGPD.

Distribución de roles

Tal y como se ha explicado, la parte reclamada, como titular de la página web, adoptó la decisión de implementar las Herramientas de Facebook Business en su sitio web ***URL.1. En particular, insertó un código JavaScript, proporcionado por Meta Platforms, Inc, en el código fuente de su página web, por lo que este código JavaScript

fue ejecutado en el navegador de quienes visitan la página web (entre otros, la parte reclamante) durante su visita a la misma.

En su respuesta de 11 de diciembre de 2020, la parte reclamada manifestó que había implementado Facebook Pixel y Facebook Login en ***URL.1.

Como resultado, la parte reclamada decidió sobre las finalidades y medios del tratamiento de datos relacionados con la herramienta, por lo que la parte reclamada debe ser considerado responsable de tratamiento de acuerdo con el artículo 4.7 del RGPD.

En cuanto al rol de Meta Platforms, Inc, a pesar de las extensas actuaciones de investigación, esta Agencia no ha encontrado evidencias suficientes para calificar a Meta Platforms, Inc como responsable del tratamiento.

Por tanto, esta Agencia asume, por lo tanto, que al menos desde el 21 de agosto de 2020 Meta Platforms, Inc actuó como subencargado de tratamiento de la parte reclamada, de conformidad con el artículo 28, apartado 2, del RGPD.

Ámbito de aplicación del capítulo V del RGPD

La parte reclamada está establecida en España y es titular de la página web ***URL.1, la cual se encuentra en el ámbito de aplicación del RGPD. Además, la parte reclamada ha compartido los datos personales de quienes visitan su página web (entre otros, de la parte reclamante) con Meta Platforms, Inc proactivamente al implementar las Herramientas de Facebook Business en su página web ***URL.1.

Meta Platforms, Inc se encuentra ubicada en Estados Unidos. No ha sido posible determinar si los datos personales de quienes visitan la página web (entre otros, de la parte reclamante) fueron transmitidos directamente a Meta Platforms Inc, o solo después de haber sido tratados por Meta Ireland.

De acuerdo con el artículo 28.1 del RGPD, la parte reclamada está obligada a cooperar solo con encargados que provean garantías suficientes de que el tratamiento de datos se realiza de acuerdo con los requisitos del RGPD.

En el presente caso, la parte reclamada aceptó los términos y condiciones de las Herramientas para Empresas de Facebok Irlanda y, de acuerdo con el artículo 28.2 del RGPD, acordó que Meta Irlanda pudiera usar a Meta Platforms, entre otros, como subencargado de tratamiento.

De acuerdo con las Directrices 05/2021 sobre la interacción entre la aplicación del artículo 3 y las disposiciones sobre transferencias internacionales de conformidad con el capítulo V del RGPD del CEPD, el mero tratamiento o la participación de una persona jurídica de EEUU ya equivale a la existencia de una transferencia en el sentido del Capítulo V del RGPD. En el presente caso, la parte reclamada no demostró si transfirió o no datos directamente a EEUU- aunque se exige responsabilidad proactiva por cada tratamiento en virtud del artículo 5.2 del RGPD.

Sin embargo, esto no es relevante toda vez que la parte reclamada era el responsable del tratamiento a través de toda la cadena de tratamiento y- dado que los datos terminan siendo tratados por una empresa de EEUU y en EEUU- la parte reclamada, por tanto, está obligada a cumplir con el artículo 44 del RGPD. En especial, la referencia de la parte reclamada al Ejemplo 1 de las Directrices 05/2021 no es correcta ya que no existe una recogida directa en este caso sino un tratamiento inducido y hecho posible por la parte reclamada (el responsable del tratamiento) al integrar los servicios de Facebook (tal y como se ha descrito anteriormente en la referencia a la sentencia Fashion ID).

En el presente caso, la parte reclamada aceptó las condiciones de las Herramientas de Facebook Business de Meta Ireland para el tratamiento de datos y, de acuerdo con el Artículo 28.2 del RGPD, acordó que Meta Ireland, pudiera, entre otros, utilizar a Meta Platforms, Inc. como subencargado de tratamiento.

Por tanto, resulta necesario comprobar si las transferencias de datos personales a Estados Unidos tuvieron lugar de acuerdo con lo dispuesto en el Capítulo V del RGPD.

El artículo 44 "*Transferencias de datos personales a terceros países u organizaciones internacionales*" del RGPD establece:

"Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

Es decir, el capítulo V del RGPD prevé diversos instrumentos para garantizar un nivel de protección sustancialmente equivalente al garantizado en la Unión Europea, de conformidad con el artículo 44 del Reglamento, a saber:

- decisiones de adecuación (artículo 45);

- garantías adecuadas (artículo 46);

A falta de un nivel de protección equivalente, establece excepciones para situaciones específicas (artículo 49).

i) Decisión de adecuación (artículo 45 del RGPD)

Al menos hasta el 10 de julio de 2023 la parte reclamada y Meta Platforms, Inc se basaban en la Decisión de adecuación EU-US ("Privacy Shield") de 2016 para realizar las citadas transferencias internacionales de datos personales.

Sin embargo, el TJUE en su sentencia de 16 de julio de 2020, C-311/18, declaró que tal decisión de adecuación no garantizaba un nivel adecuado de protección para las

personas físicas debido a la normativa de Estados Unidos pertinente y a la implementación de programas oficiales de vigilancia basados, entre otros, en la Sección 702 de FISA y E.O.12333 en conjunto con PPD-28 y anuló la citada decisión de adecuación.

Esta Agencia entiende que Meta Platforms, Inc debe ser calificado como proveedor de servicios de comunicaciones electrónicas en el sentido del Código U.S. 50 § 1881(b)(4), por lo que estaba sujeto a vigilancia por las autoridades de inteligencia de Estados Unidos, de conformidad con el Código de los EE.UU. 50 § 1881.a («FISA 702»).

Por tanto, Meta Platforms, Inc tenía la obligación de proporcionar a las autoridades de Estados Unidos los datos personales de conformidad con el artículo 1881.a del Código de los EE.UU.

ii) Garantías adecuadas

La parte reclamada tampoco podía basar la transferencia de datos en las cláusulas contractuales tipo de protección de datos previstas en Artículo 46(2)(c) y (d) del RGPD si el tercer país de destino no garantizaba una protección adecuada, con arreglo a la legislación de la UE, de los datos personales transferidos con arreglo a esas cláusulas (ver los párr. 134 y 135 de la Sentencia). El TJUE ha fallado explícitamente que las transferencias ulteriores a empresas comprendidas en el artículo 50 del EEUU Código "U.S. Code") § 1881a no sólo violan los artículos pertinentes del Capítulo V del RGPD, sino también los artículos 7 y 8 de la CFR, así como la esencia del artículo 47 de la CFR (ver C-362/14 ("Schrems I"), párr. 95.) Por lo tanto, toda transferencia ulterior viola el derecho fundamental a la privacidad, la protección de los datos y el derecho a la tutela judicial efectiva y a un juez imparcial.

Meta Platforms Inc. se califica como un proveedor de servicios electrónicos en el sentido del 50 U.S. Code § 1881(b)(4) y como tal está sujeto a la vigilancia de la inteligencia de los Estados Unidos en virtud del 50 U.S. Code § 1881a ("FISA 702"). Como se desprende del propio "Transparency Report" del Facebook (ver https://transparency.facebook.com/government-data-requests/country/US) Facebook está proporcionando activamente datos personales al gobierno de los EEUU bajo el 50 U.S. Code § 1881a.

Como consecuencia, la parte reclamada no podía garantizar una protección adecuada de los datos personales de quienes visitaban su página web (entre otros, de la parte reclamante) que se transferían a Meta Platforms Inc. Por lo tanto, la parte reclamada tenía la obligación legal de abstenerse de transferir los datos de quienes visitaban su página web (entre otros, de la parte reclamante) - o cualquier otro dato personal- a Meta Platforms Inc.

iii) Excepciones para determinados casos

Esta Agencia considera que no se cumple ningún requisito de los del artículo 49 del RGPD y, en particular, no se ha obtenido ningún consentimiento de acuerdo con el artículo 49.1.a).

Por todo lo anteriormente expuesto, esta Agencia entiende que las transferencias internacionales de datos personales de la parte reclamada a Meta Platforms Inc, no estaba cubierta por ningún instrumento del artículo 45 y siguientes del RGPD.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de resolución de procedimiento de apercibimiento, se considera que los hechos conocidos son constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 44 del RGPD.

V
Tipificación y calificación de la infracción del artículo 44 del RGPD

El artículo 83.5.c) del RGPD tipifica como infracción la vulneración de las disposiciones siguientes:

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;
(…)"

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
(…)
l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679. (…)"

VI
Apercibimiento

El artículo 64 de la LOPDGDD que regula la "*Forma de iniciación del procedimiento y duración"*, en su apartado tercero dispone que:

"3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.
El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo."

En el presente caso, considerando las circunstancias enumeradas en el artículo 83.2 RGPD, se considera conforme a derecho dirigir un apercibimiento a la parte reclamada.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DIRIGIR UN APERCIBIMIENTO a **FREEPIK COMPANY S.L.**, con NIF B93183366, por una infracción del Artículo 44 del RGPD, tipificada en el Artículo 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a **FREEPIK COMPANY S.L**.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

1403-16012024

Mar España Martí

Directora de la Agencia Española de Protección de Datos