Expediente N.º: EXP202300665 (PA/00052/2023)

RESOLUCIÓN DE PROCEDIMIENTO DE APERCIBIMIENTO

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 29 de noviembre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **FÁBRICA NACIONAL DE MONEDA Y TIMBRE - REAL CASA DE LA MONEDA** con NIF Q2826004J (en adelante, FNMT). Los motivos en que basa la reclamación son los siguientes:

Reclamación relacionada con la utilización de cookies por parte de la Fábrica Nacional de Moneda y Timbre en el sitio web https://***URL.1/, sin informar ni recabar el consentimiento de los usuarios adecuadamente. Se hace mención específica a la utilización de cookies analíticas de Google (GA) y a la posibilidad de que ello implique transferencia internacional de datos a EE. UU. Sobre estas cuestiones la parte reclamante se dirigió al DPD del organismo con fecha 17/10/22, manifestando no haber recibido respuesta.

Junto a la reclamación se aporta:

- Copia de correo electrónico remitido desde la dirección ******EMAIL.1*** a la dirección ******EMAIL.2*** de fecha 17/10/2022. En este correo, la parte reclamante presenta una queja a la FNMT acerca de que en su web se instalan cookies sin obtener el consentimiento conforme a lo dispuesto en el Artículo 4 (11) del RGPD, y que dos de esas cookies se proveen por Google Analytics, por lo que pregunta si se transfieren datos personales a los EE.UU.

- Informe automático de dataskydd.net relativo a la web ******URL.1*** de fecha 29/11/2022 donde constan instaladas, sin ninguna interacción con la web por parte del usuario, cookies de Google Analytics, como _ga y _gid. Asimismo, constan llamadas http al dominio ******DOMINIO.1***.

Con fecha 17 de enero de 2023, se adjuntaron las siguientes evidencias recogidas por esta Agencia:

- Impresión de “Aviso sobre Cookies” de la web ******URL.2***, de fecha 17/01/2023.

- Informe automático de la herramienta Website Evidence Collector sobre la visita a la web ******URL.1*** de fecha 17/01/2023 donde constan instaladas, sin ninguna interacción con la web por parte del usuario, cookies de Google Analytics, como _ga y _gid. Asimismo, constan llamadas http al dominio ******DOMINIO.1*** y la transmisión a este

dominio de parámetros como "sr", "cid" (valor de la cookie _ga), "dl", "dt", entre otros.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la FNMT, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, 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) mediante notificación electrónica, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 03/02/2023, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, se envió una copia por correo postal que fue notificada fehacientemente en fecha 14/02/2023. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

Con fecha 02/03/2023 se recibe en esta Agencia escrito de respuesta indicando que:

"*1.- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.*

*El día 17 de octubre tiene entrada en el correo electrónico del Delegado de Protección de Datos de la FNMT-RCM (*****EMAIL.2**) un correo de **A.A.A.**, con el siguiente contenido:*
De:** "**A.A.A.**"<**EMAIL.1**>*
Para:** *****EMAIL.2
***Fecha:** Lunes, *****FECHA.1** 21:42*
***Asunto:** Cookies página web FNMT*

Estimado/a Delegado/a de Protección de Datos de la FNMT:

*Me dirijo a usted con relación a las cookies y otras tecnologías similares utilizadas en la página web de la FNMT (*****URL.1**).*

Con base en el Artículo 4(11) del RGPD, así como su considerando 32, el consentimiento a la instalación de las referidas cookies no se obtiene de manera "libre, específica e inequívoca", puesto que no se ofrece la opción de "rechazar" las cookies ni de consentir o no el uso de cada una de ellas. De hecho, el cookie banner informa de que "si continúa navegando, consideramos que acepta su uso", lo cual no constituye un "acto afirmativo claro de la voluntad" del usuario de consentir a ese tratamiento de los datos personales.

Por otro lado, he podido observar que al menos dos de las cookies utilizadas en la web son proveídas por Google Analytics, por lo que me pregunto si se transfieren datos personales a Estados Unidos, considerando las recientes revelaciones acerca de Google Analytics.

Muchas gracias de antemano por considerar mis observaciones
Un saludo

A.A.A.

*Si bien la consulta de **la interesada** constaba en nuestros registros y se ha estado trabajando sobre ella se han producido las siguientes circunstancias que han impedido contestar a la misma dentro de los plazos establecidos por la norma:*

*1) Realización de varios procesos de auditoría durante el transcurso del plazo de contestación a la consulta de **la interesada** en los que ha sido requerido el Delegado de Protección de Datos de forma recurrente.*
2) Modificación del sistema para el ejercicio de derechos sobre datos personales por parte de los interesados y que ha supuesto un incremento exponencial de solicitudes sin que se hayan incrementado los recursos humanos y materiales para darles respuesta.
3) Reestructuración interna y cambios de personal dentro de la entidad que han dificultado la continuidad en la tramitación de consultas y consecuente retraso.
4) Falta de recursos personales para dar soporte al DPD-FNMT en su actividad habitual.

2.- Informe, si procede, sobre las medidas adoptadas para adecuar la política de privacidad al artículo 13 del RGPD, fechas de implantación y controles adecuados para comprobar su eficacia.

La información sobre privacidad se encuentra accesible en la página web de la FNMT-RCM y es de acceso libre a cualquier interesado a través del siguiente enlace:
******URL.1***

Controles adecuados para comprobar su eficacia

Se realizan actualizaciones periódicas sobre la política de privacidad, especialmente en lo referido al artículo 13 del RGPD. Está publicado en la página web el Registro de Actividades del Tratamiento que se revisa una vez al año salvo modificaciones en los tratamientos que requieran de su revisión actualización con otra periodicidad menor.

Realización de diferentes auditorías internas y externas (de tercera parte) relacionadas con el tratamiento de datos personales con una periodicidad anual o bianual, dependiendo de la naturaleza y requisitos de las mismas y el tipo de certificación asociada.

3.- Informe, si procede, sobre las medidas adoptadas para adecuar la utilización de cookies a lo dispuesto en el artículo 22.2 de la Ley 34/2002, de 11 de julio, (LSSI), en particular sobre la información facilitada a los usuarios sobre la utilización de cookies y los fines del tratamiento de los datos, así como la forma de recabar, rechazar o retirar

el consentimiento para su uso. Se pide además indicación de fechas de implantación y controles efectuados para comprobar su eficacia.

En estos momentos se está realizando un proceso de migración de la página web de la FNMT-RCM. Dentro de los cambios que se van a realizar se encuentran las siguientes acciones previstas:

- Incorporar la opción de otorgar o rechazar las cookies dando sólo el consentimiento de aquellas que el usuario considere dentro de los límites de la normativa a este respecto.

- Abordar un cambio a Google Analytics 4 u otro sistema compatible con Liferay que permita seguir monitorizando la página web de la FNMT-RCM dentro de los límites de la legalidad vigente.

Fechas de implantación
Las medidas anteriormente indicadas tienen como previsión estar implantadas dentro del segundo trimestre del presente año 2023."

Controles para comprobar su eficacia

Revisiones internas periódicas para monitorizar por la entidad del cumplimiento de los diferentes aspectos de la privacidad de la información y protección de datos dentro de la Entidad Realización de diferentes auditorías internas y externas (de tercera parte) relacionadas con el tratamiento de datos personales con una periodicidad anual o bianual, dependiendo de la naturaleza y requisitos de las mismas y el tipo de certificación asociada.

4.- La decisión adoptada a propósito de esta reclamación.

Realizar las actuaciones indicadas en los puntos anteriores.
*Emitir contestación a la interesada, **A.A.A.**, en los términos requeridos.*

5.- Cualquier otra que considere relevante.

No se realizan más aportaciones por parte de esta FNMT-RCM."

TERCERO: Con fecha 28 de febrero de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 27 de octubre 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 83.5 del RGPD.

QUINTO: 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 entrega mediante correo postal en fecha 8 de noviembre de 2023, como consta en el acuse de recibo que obra en el expediente.

SEXTO: Una vez transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la FNMT.

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: ***A.A.A.*** (la parte reclamante) el 14/10/2022 a las 21:42 horas, envió un correo electrónico a la dirección ******EMAIL.2***, siendo ésta la dirección del Delegado de Protección de Datos de la FNMT. Entre otras cuestiones, la parte reclamante planteaba lo siguiente:

"(…) Por otro lado, he podido observar que al menos dos de las cookies utilizadas en la web son proveídas por Google Analytics, por lo que me pregunto si se transfieren datos personales a Estados Unidos, considerando las recientes revelaciones acerca de Google Analytics."

SEGUNDO: De acuerdo las evidencias recogidas por esta Agencia el 17/01/2023, en el informe automático de la herramienta Website Evidence Collector sobre la visita a la web ******URL.1***, sin ninguna interacción con la web por parte del usuario, constan instaladas cookies de Google Analytics, como _ga y _gid. Asimismo, constan llamadas http al dominio ***DOMINIO.1 y la transmisión a este dominio de parámetros como "sr", "cid" (valor de la cookie _ga), "dl", "dt", entre otros; se establecieron los siguientes números de identificación de usuario en las cookies «_ga» y «_gid» para la posterior transmisión a Google:

Dominio	Nombre	Valor	Finalidad
https://***URL.1/	_ga	***XXXXXXXXXXXXXXXX***	Google Analytics
https://***URL.1/	_gid	***XXXXXXXXXXXXXXXX***	Google Analytics

TERCERO: Conforme a las evidencias recogidas por esta Agencia el 17/01/2023 en el informe automático de la herramienta Website Evidence Collector, FNMT ha introducido el código de la herramienta Google Analytics en su sitio web ******URL.1***.

CUARTO: Según consta en la respuesta a la pregunta 4 (ii) del documento de 09 de abril de 2021 de GOOGLE LLC obrante en el expediente, el propietario del sitio web que tenga implementado en dicha web el código de Google Analytics, puede elegir entre múltiples períodos de retención que oscilan entre 2 meses y 50 meses desde el momento en que se recopilaron los datos.

QUINTO: Según el "Aviso sobre Cookies" de la FNMT (página 12 del expediente), obtenido en las actuaciones realizadas por esta Agencia con fecha 17/01/2023, las cookies de Google Analytics tienen el siguiente plazo de caducidad en días:

- Cookie "_ga": 730 días.
- Cookie "_gid": 1 día.

SEXTO: A 24 y 25 de marzo de 2022, en la descripción de Google Analytics localizable en las urls ***URL.3 y ***URL.4 constaba, entre más información, que las cookies _ga y _gid se usaban para distinguir usuarios y que el parámetro "sr" se refería a la resolución de pantalla.

SÉPTIMO: Según el "Aviso sobre Cookies" de la FNMT (página 7 del expediente), obtenido en las actuaciones realizadas por esta Agencia con fecha 17/01/2023, las cookies de Google Analytics son del tipo "*Persistente*" y, según "*se utiliza para saber por donde navegan los usuarios*". Los datos se circunscriben a cómo los usuarios, mediante sus dispositivos, interactúan con el sitio web de la FNMT (datos de navegación internos al sitio web).

OCTAVO: El 27 de octubre de 2021, el plenario del Comité Europeo de Protección de datos de fecha 2 de septiembre de 2020, decidió crear un grupo de trabajo para asegurar una aproximación coherente entre las autoridades de datos europeas para gestionar las 101 reclamaciones relativas a que el responsable de tratamiento había embebido código de servicios de Google o Facebook, mediante los cuales se habían transferido sus datos personales a Estados Unidos, sin tener base jurídica para ello.

NOVENO: En el documento de fecha 9 de abril de 2021. remitido por GOOGLE LLC a la autoridad austríaca de protección de datos, la cual lo comparte con el resto de las autoridades a través del Grupo de trabajo para las 101 reclamaciones de NOYB en el contexto de la sentencia del TJUE Schrems II ("101 Taskforce", en adelante, grupo de trabajo TF101), consta la siguiente información y manifestaciones (de su traducción no oficial del inglés):

(...)

DÉCIMO: En el modelo de Contrato de adhesión a los servicios de GOOGLE, con el título "*Términos del Tratamiento de Datos de Google Ads*" (***URL.5**), en su versión de 21 de septiembre de 2022, constaba que:

"Términos del Tratamiento de Datos de Google Ads

Google y la contraparte que acepta las presentes Condiciones (el "Cliente"), han celebrado un contrato para la prestación de los Servicios del encargado del tratamiento (con sus enmiendas puntuales, el "Contrato")

Las presentes Condiciones del tratamiento de datos de los anuncios de Google, (las "Condiciones del tratamiento de datos") se suscriben por Google y el Cliente y complementan al Contrato.

[…]

Si usted acepta estos Términos del Tratamiento de Datos en nombre del Cliente, usted garantiza que a) tiene plena autoridad legal para que estos Términos del Tratamiento de Datos sean vinculantes para el Cliente, b) ha leído y comprende estos Términos del Tratamiento de Datos y c) los acepta en nombre del Cliente. Si no tiene la autoridad legal para que estos Términos del Tratamiento de Datos sean vinculantes para el Cliente, no los acepte.

Introducción

Estos Términos del Tratamiento de Datos reflejan el acuerdo entre las pa.es con respecto a los términos que rigen el tratamiento de determinados datos en relación con la Legislación Europea de Protección de Datos y cierta Legislación No Europea de Protección de Datos.

Definiciones e interpretación

[…]
"Entidad de Google" hace referencia a Google LLC (anteriormente conocida como Google Inc.), Google Ireland Limited o cualquier otra entidad que, directa o indirectamente, controle a Google LLC, esté controlada por Google LLC o esté sujeta al mismo control que Google LLC.

"Google": hace referencia a la Entidad de Google que sea parte del Contrato.

"Legislación Europea de Protección de Datos" hace referencia, según corresponda, a) al RGPD y/o b) a la FDPA de Suiza.
[…]

"SCCs" hace referencia a las Cláusulas Contractuales Tipo del Cliente y/o las Cláusulas Contractuales Tipo (Encargado del Tratamiento de la UE al Encargado del Tratamiento, Exportador de Google), según corresponda.
[…]

"SCCs (Encargado del Tratamiento al Encargado del Tratamiento, Exportador de Google)" hace referencia a los términos incluidos en ******URL.6****.*
[…]

" Subencargados del Tratamiento" hace referencia a terceros autorizados en virtud de estos Términos del Tratamiento de Datos para tener acceso lógico a los Datos Personales del Cliente y tratarlos con la finalidad de prestar parte de los Servicios del Encargado del Tratamiento y cualquier asistencia técnica relacionada.

[…]

5. Tratamiento de datos

5.1 Roles y cumplimiento normativo; autorización.

5.1.1 Responsabilidades del Encargado del Tratamiento de Datos y del Responsable del Tratamiento de Datos.
Las partes reconocen y aceptan lo siguiente:

El apéndice 1 describe la cuestión y los detalles del tratamiento de Datos Personales del Cliente.
(b)Google es un encargado del tratamiento de datos personales del Cliente;
(c) El Cliente es un responsable del tratamiento de datos o un encargado del tratamiento, según corresponda, de los Datos Personales del Cliente; y
(d)Cada parte cumplirá las obligaciones que le correspondan en virtud de la Legislación Aplicable de Protección de Datos con respecto al tratamiento de Datos Personales del Cliente.

[…]

5.2. Instrucciones del Cliente. Al suscribir los presentes Términos del Tratamiento de Datos, el Cliente indica a Google que trate los Datos Personales del Cliente únicamente de conformidad con la ley aplicable: a) para prestar los Servicios del Encargado del Tratamiento y cualquier asistencia técnica relacionada, b) tal y como se especifica más detalladamente a través del uso por parte del Cliente de los Servicios del Encargado del Tratamiento (incluidas la configuración y otras funciones de los Servicios del Encargado del Tratamiento) y cualquier asistencia técnica relacionada, c) según se documenta por medio del Contrato (incluidos estos Términos del Tratamiento de Datos) y d) tal y como se documenta más detalladamente en otras instrucciones proporcionadas por escrito por el Cliente y reconocidas por Google como instrucciones constitutivas para los propósitos de estos Términos del Tratamiento de Datos (en conjunto, las "Instrucciones").

5.3 Cumplimiento de las Instrucciones por parte de Google. Google cumplirá las Instrucciones a menos que lo prohíban las Leyes Aplicables o dichas Leyes Aplicables exijan otro tratamiento.

[…]

10. Transferencias de datos

10.1 Almacenamiento de datos e instalaciones de tratamiento. De conformidad con esta sección 10 (Transferencias de datos), Google podrá tratar Datos Personales del Cliente en cualquier país en el que Google o cualquiera de sus Subencargados del Tratamiento tenga instalaciones.

10.2 Transferencias Europeas Restringidas. Las partes reconocen que la Legislación Europea de Protección de Datos no exige SCCs ni una Solución Alternativa de Transferencia para tratar Datos Personales del Cliente en un País Adecuado ni para transferirlos a este. Si los Datos Personales del Cliente son transferidos a cualquier otro país y a esas transferencias se les aplica la Legislación Europea de Protección de Datos ("Transferencias Europeas Restringidas"), en ese caso:

Si Google adopta una Solución Alternativa de Transferencia para cualquier Transferencia Europea Restringida, Google informará al Cliente de la solución

relevante y se asegurará de que dichas Transferencias Europeas Restringidas se realicen de acuerdo con dicha Solución y/o Si Google no ha adoptado o ha informado al Cliente de que ya no va a adoptar ninguna Solución Alternativa de Transferencia para ninguna Transferencia Europea Restringida, en ese caso:

Si la dirección de Google se encuentra en un País Adecuado:

Se aplicarán las SCCs del Encargado del Tratamiento al Encargado del Tratamiento, Exportador de Google) con respecto a todas las Transferencias Europeas Restringidas de Google a los Subencargados del Tratamiento y.

(B) Además, si la dirección del Cliente no se encuentra en un País Adecuado, se aplicarán las SCCs (Encargado del Tratamiento al Responsable del Tratamiento de Datos) con respecto a las Transferencias Europeas Restringidas entre Google y el Cliente, independientemente de si el Cliente es un responsable y/o un encargado del tratamiento o

(ii) Si la dirección de Google no se encuentra en un País Adecuado, Se aplicarán las SCCs del Responsable del Tratamiento de Datos al Encargado del Tratamiento y/o las SCCs (Encargado del Tratamiento al Encargado del Tratamiento), en función de si el Cliente es un responsable del tratamiento de datos y/o un encargado del tratamiento, con respecto a las Transferencias Europeas Restringidas entre el Cliente y Google.

10.3 Medidas complementarias e información. Google proporcionará al Cliente la información pertinente sobre las Transferencias Europeas Restringidas, incluida la información sobre medidas complementarias para proteger los Datos Personales del Cliente, tal y como se describe en la sección 7.5.1 (Revisiones de la Documentación de Seguridad), en el apéndice 2 (Medidas de Seguridad) y en otros materiales relacionados con la naturaleza de los Servicios del Encargado del Tratamiento y con el tratamiento de los Datos Personales del Cliente (por ejemplo, artículos del centro de ayuda).

10.4 Resolución. Si el Cliente concluye, según el uso que hace o pretende hacer de los Servicios del Encargado del Tratamiento, que la Solución Alternativa de Transferencia y/o las SCCs, según corresponda, no proporcionan la protección adecuada para los Datos Personales del Cliente, el Cliente podrá resolver inmediatamente el Contrato por conveniencia mediante una notificación por escrito a Google.

10.5 Información de centros de datos. La información sobre las ubicaciones de los centros de datos de Google está disponible en ******URL.7.***

11. Subencargados del tratamiento de datos.

11.1 Consentimiento de contratación de un Subencargado del Tratamiento. El Cliente autoriza específicamente la contratación como Subencargados del Tratamiento de las entidades que figuren, a partir de la Fecha de Entrada en Vigor de los Términos, en la URL especificada en la sección 11.2 (Información sobre los Subencargados del Tratamiento). Asimismo, y sin perjuicio de lo estipulado en la sección 11.4 (Oportunidad de oponerse a cambios del Subencargado del Tratamiento), el Cliente

autoriza de forma general la contratación de cualquier otro tercero como Subencargado del Tratamiento ("Nuevos Subencargados del Tratamiento").

[…]" (el subrayado es nuestro).

UNDÉCIMO: A 5 de febrero de 2024 en la url ******URL.8*** constaba (traducción no oficial, original en inglés):

"[…]
Solicitudes de agencias gubernamentales de EE. UU. en casos que involucran seguridad nacional

En investigaciones relacionadas con la seguridad nacional, el gobierno de los EE. UU. puede utilizar una Carta de Seguridad Nacional (NSL) o una de las autorizaciones otorgadas en virtud de la Ley de Vigilancia de Inteligencia Extranjera (FISA) para obligar a Google a proporcionar información del usuario.

Una NSL no requiere autorización judicial y solo puede usarse para obligarnos a proporcionar información limitada del suscriptor.

Las órdenes y autorizaciones de FISA se pueden usar para obligar a la vigilancia electrónica y la divulgación de datos almacenados, incluido el contenido de servicios como Gmail, Drive y Photos."

[…]" (traducción no oficial, original en inglés)

DUODÉCIMO: A 5 de febrero de 2024 en la url ******URL.9*** constaba (traducción no oficial, original en inglés):

"[…]

Conceptos básicos sobre la información personal identificable en los contratos y las políticas de Google.

En muchos contratos, términos del servicio y políticas de los productos de publicidad y medición de Google se hace referencia a la "información personal identificable" (IPI). Se trata de una categorización de datos diferente a lo que el Reglamento General de Protección de Datos (RGPD) considera "datos personales".

Tenga en cuenta que, aunque Google no identifique ciertos datos como información personal identificable, es posible que el RGPD sí lo haga o que esos datos se consideren información personal de conformidad con la Ley de Privacidad del Consumidor de California (CCPA), y pueden estar sujetos a esas leyes.
[…]
Google considera "información personal identificable" la información que se pueda usar por sí sola para identificar o ubicar con precisión a una persona, o para ponerse en contacto con ella de forma directa. Entre otros datos, incluye lo siguiente:
• Direcciones de correo electrónico
• Direcciones de correo postal

• Números de teléfono
• Ubicaciones precisas (por ejemplo, coordenadas GPS, salvo en los casos que se mencionan más abajo)
• Nombres completos (nombre y apellidos) o nombres de usuario.
[…]
Entre otros, Google no considera información personal identificable los siguientes datos:
• ID de cookie seudónimos
• ID de publicidad seudónimos
• Direcciones IP
• Otros identificadores de usuario final seudónimos
Por ejemplo, si se envía una dirección IP con una solicitud de anuncio (algo que sucede con casi todas las solicitudes de anuncios como consecuencia de los protocolos de Internet), ese envío no incumplirá ninguna prohibición relacionada con el envío de información personal identificable a Google.
Tenga en cuenta que, aunque Google no identifique ciertos datos como información personal identificable, es posible que el RGPD, la CCPA u otras leyes de privacidad los consideren datos personales o información personal.
[…]"

DECIMOTERCERO: A 27 de octubre de 2023, en la url ******URL.10*** constaba la existencia de solicitudes de información FISA (Foreign Intelligence Surveillance Act) y NSL (National Security Letters) dirigidas a GOOGLE sobre información de usuarios.

FUNDAMENTOS DE DERECHO

I
Competencia y procedimiento

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 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 la naturaleza de los hechos que han dado lugar a las actuaciones y a las circunstancias concurrentes, 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 FNMT realiza la recogida y tratamiento a través del servicio Google Analytics de, entre otros, los siguientes datos personales de personas físicas: identificadores únicos de usuarios (_ga y _gid), la dirección IP, así como otros datos asociados al navegador y a la propia navegación, entre otros tratamientos.

FNMT 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. La determinación de la FNMT como responsable del tratamiento en cuestión se detalla en el Fundamento de Derecho III.

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

III
Transferencias de datos personales a terceros países

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".

El capítulo V del Reglamento 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:

- decisiones de adecuación (artículo 45);

- garantías adecuadas (artículo 46);

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

1. Sobre el tratamiento de datos y la responsabilidad del tratamiento.

En el documento de fecha 9 de abril de 2021 enviado por Google LLC a la autoridad

austríaca de protección de datos, el cual ésta compartió con el resto de las autoridades en el marco del grupo de trabajo para las 101 reclamaciones de NOYB, se indica que Google Analytics funciona incluyendo un bloque de código Javascript en las páginas de un sitio web. ***(…)*** para Google Analytics. La operación de 'tracking' envía datos acerca de la página solicitada a través de varios medios y envía esta información al servidor de Analytics ***(…).*** Los datos entonces se procesan más extensamente y terminan en los reportes del propietario de la web, en este caso la FNMT. Los datos que Google Analytics recolecta en beneficio del propietario de la web viene de las siguientes fuentes:

i. La petición HTTP del usuario.

Una petición HTTP contiene detalles como el navegador y el ordenador que hace la petición, como el hostname, el tipo navegador, 'referer', e idioma.

ii. Información del navegador y del sistema.

iii. Cookies de primera parte.

Los administradores de sitios web que integran el servicio de Google Analytics pueden enviar instrucciones a Google para el procesamiento de los datos recopilados a través de Google Analytics. El administrador del sitio web puede aplicar diferentes configuraciones, por ejemplo, con respecto al período de retención de datos. La función Google Analytics también permite a los administradores de sitios web monitorear y mantener la estabilidad de su sitio web, por ejemplo, manteniéndolos informados de ciertos eventos como un pico en la audiencia o el hecho de que no hay tráfico en absoluto. Google Analytics también permite a los administradores de sitios web medir y optimizar la efectividad de las campañas publicitarias realizadas utilizando otras herramientas de Google.

Por lo tanto, Google Analytics recopila la consulta http del usuario y la información sobre el navegador y el sistema operativo del usuario, entre otras cosas. Una solicitud http, para cualquier página, contiene detalles del navegador y del dispositivo que realiza la consulta, como el nombre de dominio y la información del navegador, como su tipo, referencia e idioma. Google Analytics almacena y lee cookies en el navegador del usuario para evaluar la sesión del usuario y otra información sobre la consulta.

Por lo que se refiere a estas transferencias de datos, el contrato relativo a la función Google Analytics ("Condiciones del Servicio de Google Analytics") incorpora un apéndice titulado "Términos del Tratamiento de Datos de Google Ads" (en versiones anteriores con el nombre de "Condiciones del Tratamiento de Datos de Google Ads"). Este apéndice contiene las Cláusulas Contractuales Tipo que rigen la transferencia de datos personales a los Estados Unidos de América bajo el servicio Google Analytics. Además, Google ha implementado medidas legales, organizativas y técnicas adicionales para regular las transferencias de datos bajo el servicio Google Analytics.

De conformidad con el punto 10 de los "Términos del Tratamiento de Datos de Google Ads", el responsable del tratamiento ha acordado que Google pueda almacenar y tratar datos personales del cliente (en el presente caso, datos personales de la parte reclamante) en cualquier país en el que Google o cualquiera de sus subencargados de

tratamiento de datos mantengan instalaciones. Cuando se recopila esta información, se transmite a los servidores de Google Analytics.

Volviendo al documento enviado por Google LLC con fecha 9 de abril de 2021, en el último párrafo a la respuesta de la pregunta 8, Google manifiesta que todos los datos recopilados a través de Google Analytics están alojados en los Estados Unidos. Por lo tanto, los datos recopilados en el sitio web ***«***URL.1»*** a través de Google Analytics se transfieren a los Estados Unidos. Dicha transmisión de datos requiere una base jurídica de conformidad con el artículo 44 y siguientes del RGPD.

Todos estos elementos muestran que, al decidir implementar la función de Google Analytics en su sitio web, FNMT, que gestiona el sitio web ***«***URL.1»***, determinó los medios y fines de la recopilación y el tratamiento de los datos obtenidos a raíz de la integración de Google Analytics en su sitio web y debe considerarse el responsable del tratamiento en el sentido del artículo 4.7 del RGPD.

2. Sobre la calificación de los datos objeto de tratamiento como datos personales

Puede afirmarse que los datos recopilados con arreglo a la función Google Analytics y transferidos a los Estados Unidos de América constituyen datos personales.

El artículo 4.1 del RGPD define los datos personales *como «toda información relativa a una persona física identificada o identificable («el interesado»); una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador, como un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o varios factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física*.».

Cabe señalar que los identificadores en línea, como las direcciones IP o la información almacenada en las cookies, pueden utilizarse comúnmente para identificar a un usuario, especialmente cuando se combinan con otros tipos de información similares. Esto se ilustra en el considerando 30 del RGPD, según el cual la asignación de identificadores en línea como direcciones IP, identificadores de cookies a personas físicas o sus dispositivos pueden *«dejar rastros que, en particular cuando se combinan con identificadores únicos y otra información recibida por los servidores, pueden utilizarse para crear perfiles de las personas físicas e identificarlos*». En el caso particular en el que el responsable del tratamiento alegara no tener la capacidad de identificar al usuario mediante el uso (solo o combinado con otros puntos de datos) de dichos identificadores, se esperaría que revelara los medios específicos desplegados para garantizar el anonimato de los identificadores recopilados. Sin tales detalles, no pueden considerarse anónimos.

Por lo tanto, es necesario examinar en qué medida la implementación de Google Analytics en un sitio web permite al administrador del sitio web y a Google hacer que un interesado (un visitante del sitio web en cuestión) pueda identificarse.

Cuando la parte reclamante visitó el sitio web ******URL.1***, los siguientes datos (a través del código JavaScript) fueron transmitidos desde el navegador de la parte reclamante a los servidores de Google LLC:

- Cookies _ga y _gid
- URL de la página web visitada (parámetro dl) y título de la página web visitada (parámetro dt)
- IP
- sr (resolución de pantalla), entre otros parámetros.
- Datos sobre el navegador y sistema operativo:
- Identificador único que identifica al operador del sitio web

Cabe señalar que el TJUE ya ha declarado que las direcciones IP son datos personales (véase el asunto C-597-19, punto 102 y C-582/14, punto 49). La dirección IP no pierde su naturaleza de datos personales simplemente porque los medios de identificación residen en terceras entidades. Además, el caso en cuestión es muy diferente, ya que la dirección IP puede combinarse con otros elementos, como se describirá a continuación.

En lo que respecta a los identificadores únicos, cuando un usuario visita el sitio web ***URL.1, según el informe de Website Evidence Collector de fecha 17 de enero de 2023, se establecieron los siguientes números de identificación de usuario en las cookies «_ga» y «_gid» y posteriormente se transmitieron a Google LLC:

Dominio	Nombre	Valor	Finalidad
https://***URL.1/	_ga	***XXXXXXXXXXXXXXX***	Google Analytics
https://***URL.1/	_gid	***XXXXXXXXXXXXXXX***	Google Analytics

Según la descripción de Google Analytics localizable en las urls:
"******URL.3***"
y "******URL.4***"
, las cookies _ga y _gid se usan para distinguir a los usuarios y que el parámetro "sr" se refiere a la resolución de pantalla.

Los identificadores de visitantes son identificadores únicos destinados para diferenciar a individuos (donde esa diferenciación no era posible antes), y hacen que los individuos sean identificables. Estos identificadores también pueden combinarse con otra información, como la dirección del sitio web visitado, los metadatos relativos al navegador y el sistema operativo, la hora y los datos relativos a la visita al sitio web y la dirección IP. Esta combinación de información diferencia aún más a los individuos.

Por esta razón, cuando se combinan varios elementos, pueden permitir identificar individualmente a los visitantes de la página web de «******URL.1***», en la que se implementa Google Analytics. No es necesario conocer el nombre o la dirección (física) del visitante, ya que, de acuerdo con el considerando 26 del RGPD, tal calificación de las personas es suficiente para que el visitante sea identificable.

Si se decidiera lo contrario, el alcance del derecho a la protección de datos, garantizado por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, se vería socavado, ya que permitiría a las empresas seleccionar específicamente a las personas junto con la información personal (por ejemplo, cuando visitan un sitio web específico) al mismo tiempo que les negaría cualquier derecho de protección contra tal singularización. Una opinión tan restrictiva que socavaría el nivel de protección de las personas tampoco está en consonancia con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), que dictaminó repetidamente que el ámbito de aplicación del RGPD debe entenderse de manera muy amplia (véase, por ejemplo, la sentencia C-439/19, apartado 61).

Google LLC afirma que no tiene «ninguna intención» de utilizar identificadores en línea para identificar a la parte reclamante (u otras personas), según refiere en el último párrafo de la respuesta a la pregunta 13 del documento de 9 de abril de 2021 y que de hecho «no hacen esto». Hay que señalar que el artículo 4, apartado 1, del RGPD no requiere que una entidad tenga una intención específica de identificar a una persona. De acuerdo con la redacción clara del artículo 4, apartado 1, del RGPD, el término «datos personales» se completa cuando una entidad puede (tiene la posibilidad) de hacerlo.

Aparte de esto, incluso tras una interpretación más restrictiva del artículo 4, apartado 1, del RGPD, que en cualquier caso sería contrario a la jurisdicción del TJUE, la definición de «datos personales» se entendería aplicable a los datos expuestos. En el caso de que algún visitante de la web ******URL.1*** hubiese iniciado sesión en una cuenta de Google en el momento de su visita, tal y como puede verse en la declaración de Google LLC del 9 de abril de 2021, la implementación de Google Analytics en un sitio web permite a Google recibir la información que un usuario específico de la cuenta de Google ha visitado ese sitio web.

En el contexto del uso de Google Analytics, y dependiendo de algunos ajustes en la configuración de la cuenta de usuario de Google (ver respuesta a la pregunta 9 del documento de Google de 9 de abril de 2021), permite a Google recibir información de que un usuario conectado a una cuenta de Google ha visitado un sitio web en particular. Por lo tanto, se recopilan datos personales relacionados con esta cuenta.

Por todo ello, debe considerarse que los datos en cuestión son datos personales en el sentido del artículo 4.1 del RGPD.

3. Sobre el incumplimiento de la obligación de regular las transferencias de datos personales fuera de la Unión Europea

En el presente caso, debe verificarse si produjo la exportación de datos personales a los Estados Unidos de América como señala la parte reclamante, en los términos que establece el artículo 44 del RGPD, y, en caso de que se hubiera producido, si la exportación se realizó con un nivel de protección adecuado conforme a una decisión de adecuación del artículo 45 del RGPD, o, en su defecto, si se adoptó alguna de las garantías del artículo 46 del RGPD.

a. Decisiones de adecuación

En su sentencia del asunto C-311/18 ("Schrems II"), de 16 de julio de 2020, el TJUE invalidó la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección ofrecida por el "EU-US Privacy Shield" ("Escudo de la privacidad"), sin mantener sus efectos en la fecha de los hechos objeto de reclamación.

En ausencia de decisión de adecuación vigente con los EE. UU. en el momento de los hechos, la transferencia de datos en cuestión no pudo estar basada en lo dispuesto en el artículo 45.3 del RGPD.

b. Salvaguardias apropiadas: Cláusulas tipo de protección de datos

El artículo 46, "*Transferencias mediante garantías adecuadas*", del RGPD, establece en su apartado 1 que "*A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.»*

El artículo 46, apartado 2, del RGPD dispone que "*Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:*
(…)
c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2.
(…)".

Las Cláusulas Contractuales Tipo de Google para la transferencia de datos personales a los Estados Unidos, en su versión de 21 de septiembre de 2022, con el nombre *"Google Ads & Measurement: Standard Contractual Clauses (Module 3: Processor-to-Processor)*", que podría traducirse como: "Términos de tratamiento de datos de Google Ads: Modelo de Cláusulas Contractuales, Cláusulas Contractuales Tipo Encargado a Encargado" (en adelante, SCC). Estas cláusulas se ajustan a las publicadas por la Comisión Europea en la Decisión 2010/87/UE.

En este contexto, cabe destacar que las Cláusulas Contractuales Tipo son un instrumento de transferencia en el sentido del capítulo V del Reglamento y no fueron impugnadas como tales por el TJUE en su sentencia de 16 de julio de 2020 (C-311/18). Sin embargo, el TJUE consideró que de la naturaleza contractual de estas cláusulas se derivaba que no podían ser vinculantes para las autoridades de terceros países. En particular, el TJUE declaró que: "...*Por lo tanto, si bien existen situaciones en las que, en función de la legislación y las prácticas vigentes en el tercer país de que se trate, el destinatario de dicha transferencia está en condiciones de garantizar la protección necesaria de los datos únicamente sobre la base de Cláusulas Contractuales Tipo de protección de datos, existen otras en las que el contenido de dichas cláusulas tipo podría no constituir un medio suficiente para garantizar, en la práctica, la protección efectiva de los datos personales transferidos al tercer país de que se trate. Este es el caso, en particular, cuando la legislación de ese tercer país permite a sus autoridades públicas interferir con los derechos de los interesados a los*

que se refieren dichos datos" (C-311/18, punto 126, subrayado añadido).

Sin embargo, no es necesario un análisis adicional de la situación jurídica de los Estados Unidos, ya que el TJUE ya lo ha proporcionado en su sentencia antes mencionada. En efecto, el TJUE consideró que los programas de vigilancia reglamentaria como el artículo 702 de la FISA y el E.O. 12333 en conjunción con la PPD-28, no satisfacen las exigencias mínimas establecidas por el Derecho de la Unión con respecto al principio de proporcionalidad, de modo que los programas de vigilancia basados en estas disposiciones no pueden considerarse limitados a lo estrictamente necesario (C-311/18, punto 184). Además, el TJUE consideró que el marco jurídico en cuestión no confería a los interesados derechos susceptibles de recurso ante los tribunales contra las autoridades estadounidenses, de lo que se deduce que estas personas no tienen derecho a una tutela judicial efectiva (C-311/18, punto 192).

El análisis del TJUE es pertinente en el presente asunto, ya que Google LLC (como importador de los datos a los EE. UU.) debe calificarse como proveedor de servicios de comunicaciones electrónicas en el sentido del apartado (b) del punto 4 del artículo 1881 del título 50 del Código de los Estados Unidos y, por lo tanto, está sujeto a vigilancia por parte de los servicios de inteligencia de EE. UU. de acuerdo con el apartado (a) del artículo 1881 del título 50 del Código de los Estados Unidos («FISA 702»). Por lo tanto, Google LLC tiene la obligación de proporcionar datos personales al gobierno de los Estados Unidos cuando se le solicite de conformidad con el apartado (a) del artículo 1881 del título 50 del Código de los Estados Unidos (FISA 702).

Como se puede ver en el Informe de transparencia de Google, Google LLC está sujeto regularmente a tales solicitudes de acceso por parte de los servicios de inteligencia de Estados Unidos. El informe puede consultarse en:
******URL.10***

El TJUE declaró, por un lado, que la decisión de adecuación UE-EE. UU. era inválida debido a las posibilidades de acceso de los servicios de inteligencia estadounidenses y, por otro, que la conclusión de que la utilización de las Cláusulas Contractuales Tipo no puede por sí sola garantizar un nivel de protección, tal como exige el artículo 44 del RGPD, ya que las garantías que ofrecen quedan sin cumplir cuando se realizan dichas solicitudes de acceso. De hecho, el TJUE concluyó lo siguiente:

"*De ello se deduce que las cláusulas tipo de protección de datos adoptadas por la Comisión sobre la base del artículo 46, apartado 2, letra c), del RGPD solo tienen por objeto ofrecer garantías contractuales que se aplican de manera uniforme en todos los terceros países a los responsables y encargados del tratamiento establecidos en la Unión Europea y, en consecuencia, con independencia del nivel de protección garantizado en cada tercer país. En la medida en que estas cláusulas tipo de protección de datos no pueden, habida cuenta de su propia naturaleza, ofrecer garantías más allá de una obligación contractual de garantizar el cumplimiento del nivel de protección exigido por el Derecho de la Unión, pueden exigir, en función de la posición imperante en un tercer país determinado, la adopción de medidas complementarias por parte del responsable del tratamiento para garantizar el cumplimiento de dicho nivel de protección"* (C-311/18, punto 133).

(i) Observaciones generales sobre las medidas complementarias

En sus Recomendaciones 01/2020, de 18 de junio de 2021, (que se pueden consultar en la web ******URL.11***, aunque las transcripciones incluidas en este documento se refieren a su traducción al español) el Comité Europeo de Protección de Datos (CEPD) ha aclarado que, cuando la evaluación de la legislación o las prácticas vigentes del tercer país puede afectar a la eficacia de las salvaguardias adecuadas de los instrumentos de transferencia en los que se basa el exportador, en el contexto de su transferencia específica, como sucede en este caso tras la evaluación del TJUE, el exportador debe suspender la transferencia o aplicar medidas complementarias adecuadas. El CEPD observa a este respecto que "*Cualquier medida complementaria solo podrá considerarse eficaz en el sentido de la sentencia del TJUE «Schrems II» en la medida en que aborde las deficiencias específicas detectadas en su evaluación de la situación jurídica en el tercer país. Si, en última instancia, no puede garantizar un nivel de protección esencialmente equivalente, no deberá transferir los datos personales."* (véanse las Recomendaciones 01/2020, punto 75).

Las medidas para complementar las cláusulas tipo de protección de datos pueden clasificarse en tres categorías: contractual, técnico u organizativo (véanse las Recomendaciones 01/2020, punto 74).

Con respecto a las medidas contractuales, el CEPD señaló que: "*En algunas situaciones, estas medidas pueden complementar y reforzar las garantías que el instrumento de transferencia y el Derecho pertinente del tercer país pueden proporcionar, cuando, teniendo en cuenta las circunstancias de la transferencia, estas no cumplan todas las condiciones necesarias para garantizar un nivel de protección esencialmente equivalente al garantizado en la Unión. Habida cuenta de la naturaleza de las medidas contractuales, que por lo general no pueden vincular a las autoridades de ese tercer país cuando no formen parte del contrato, estas deberán combinarse con otras medidas técnicas y organizativas para proporcionar el nivel de protección de datos requerido* (...)". (véanse las Recomendaciones 01/2020, punto 99, subrayado añadido).

Por lo que se refiere a las medidas organizativas, el CEPD destacó que: *"… Seleccionar y aplicar una o varias de estas medidas no garantizará necesaria y sistemáticamente que su transferencia cumple la norma de equivalencia esencial que exige el Derecho de la Unión. En función de las circunstancias específicas de la transferencia y de la evaluación realizada sobre el Derecho del tercer país, se necesitarán medidas organizativas para complementar las medidas contractuales o técnicas, a fin de garantizar un nivel de protección de los datos personales esencialmente equivalente al garantizado en la Unión*" (véanse las Recomendaciones 01/2020, punto 128, subrayado añadido).

Por lo que se refiere a las medidas técnicas, el CEPD señaló que «…*Estas medidas serán especialmente necesarias cuando la legislación de dicho país imponga a los importadores de datos obligaciones que sean contrarias a las garantías del artículo 46 del RGPD y puedan, en particular, afectar a la garantía contractual de un nivel de protección esencialmente equivalente contra el acceso de las autoridades públicas de ese tercer país a dichos datos*» (véanse las Recomendaciones 01/2020, punto 77). Añadió que *"Las medidas enumeradas a continuación tienen por objeto garantizar que el acceso de las autoridades públicas de terceros países a los datos transferidos no*

afecte a la eficacia de las garantías apropiadas contenidas en los instrumentos de transferencia del artículo 46 del RGPD. Estas medidas se aplican incluso si el acceso de las autoridades públicas se ajusta al Derecho del país del importador, cuando dicho acceso vaya más allá de lo necesario y proporcionado en una sociedad democrática. Estas medidas tienen por objeto evitar la posible vulneración del acceso impidiendo a las autoridades identificar a los interesados, inferir información sobre ellos, individualizarlos en otro contexto o asociar los datos transferidos con otros conjuntos de datos que puedan poseer y que puedan contener, entre otros datos, identificadores en línea proporcionados por los dispositivos, aplicaciones, herramientas y protocolos utilizados por los interesados en otros contextos." (véanse las Recomendaciones 01/2020, punto 79, subrayado añadido).

(ii) Medidas complementarias implementadas por Google LLC

Google LLC, como receptor de datos de los usuarios de sus servicios de Google Analytics, adoptó medidas contractuales, organizativas y técnicas para complementar las SCC. En el documento de fecha 9 de abril de 2021 enviado por Google LLC a la autoridad austríaca de protección de datos, la cual ésta compartió con el resto de las autoridades en el marco del Grupo de trabajo TF101, Google LLC describió las medidas adoptadas en detalle.

Teniendo en cuenta las consideraciones del TJUE y del CEPD, ahora debe verificarse si las medidas complementarias adoptadas por Google LLC eran eficaces, lo que significa que abordan la cuestión específica de las posibilidades de acceso de los servicios de inteligencia estadounidenses.

Por lo que se refiere a las "*medidas jurídicas y organizativas"* adoptadas, cabe señalar que ni la notificación de los usuarios, incluso en caso de que dicha notificación sea admisible, ni la publicación de un informe de transparencia o una «política pública sobre el tratamiento de las solicitudes gubernamentales» de hecho impiden o reducen las posibilidades de acceso de los servicios de inteligencia estadounidenses. Además, no está claro cómo la «revisión cuidadosa de cada solicitud» de Google LLC sobre su admisibilidad es efectiva como medida complementaria, teniendo en cuenta que, según el TJUE, las solicitudes (legales) admisibles de los servicios de inteligencia estadounidenses no están en consonancia con los requisitos de la normativa europea de Protección de Datos.

Con respecto a las "*medidas técnicas"* adoptadas, cabe señalar que no se ha aclarado, cómo las medidas descritas, tales como la protección de las comunicaciones entre los servicios de Google, la protección de datos en tránsito entre centros de datos, la protección de las comunicaciones entre usuarios y sitios web, o la «seguridad en el sitio», de hecho, impiden o reducen las posibilidades de acceso de los servicios de inteligencia estadounidenses sobre la base del marco jurídico de los Estados Unidos.

Por lo que se refiere a las tecnologías de cifrado, como en el caso de los «datos en reposo» en los centros de datos, como lo menciona específicamente Google LLC como medida técnica, hay que señalar que Google LLC, como importador de datos, tiene la obligación de conceder acceso o entregar datos personales importados en su poder, incluidas las claves criptográficas necesarias para que los datos sean

inteligibles (véanse las Recomendaciones 01/2020, punto 81). En otras palabras: mientras Google LLC tenga la posibilidad de acceder a los datos de las personas físicas en un texto claro, dicha medida técnica no puede considerarse efectiva en el presente caso.

En cuanto Google LLC señala que «en la medida en que los datos de Google Analytics para la medición transferidos por los propietarios de sitios web sean datos personales, habría que considerarlos como seudónimos», debe tenerse en cuenta que los identificadores únicos universales (UUID) no entran en la definición del artículo 4.5 del RGPD. Si bien la seudonimización puede ser una técnica de mejora de la privacidad, los identificadores únicos tienen, como ya se describió anteriormente, la intención específica de seleccionar a los usuarios, no de actuar como salvaguarda. Aparte de esto, también se ha descrito anteriormente por qué la combinación de identificadores únicos con otros elementos (como los datos del navegador o del dispositivo y la dirección IP) y la posibilidad de vincular dicha información a una cuenta de Google en cualquier caso hacen que una persona pueda identificarse.

En la medida en que Google LLC se refiere a una «medida técnica opcional» por medio de una función de anonimización IP, debe tenerse en cuenta, en primer lugar, que dicha medida es, como su nombre indica, opcional y no aplicable a todas las transferencias. Además, de la respuesta de Google no se desprende si esta anonimización tiene lugar antes de la transferencia o si la dirección IP completa se transmite a los Estados Unidos y solo se acorta después de esta transferencia a los Estados Unidos. Por lo tanto, desde un punto de vista técnico, existe un acceso potencial a toda la dirección IP completa antes de acortarla.

Por lo tanto, las medidas complementarias adoptadas, tal como las presentó Google, no son eficaces en la medida en que ninguna de ellas aborda las cuestiones específicas en el presente caso, lo que significa que ninguna de ellas impide las posibilidades de acceso de los servicios de inteligencia estadounidenses ni hace que estos accesos sean ineficaces.

c. Las excepciones previstas en el capítulo V del Reglamento

El artículo 49, "*Excepciones para situaciones específicas",* del RGPD establece:

"*1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:*

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

(…)"

En el presente caso, no se aprecia este ninguno de estos supuestos, teniendo en cuenta que el Considerando 111 del RGPD exige que la transferencia internacional de datos debe de ser "*ocasional y necesaria en relación con un contrato*", mientras que en este caso las transferencias se producen de forma continua y no se justifica su necesidad.

Si bien es cierto que FNMT no decide donde se conservan los datos personales por Google LLC, desde el momento en que contrata los servicios de su herramienta de Google Analytics, se entiende que está de acuerdo con el punto 10 de los "Términos del Tratamiento de Datos de Google Ads", por lo que el responsable del tratamiento ha acordado que Google pueda almacenar y tratar datos personales del cliente (es decir, datos personales de la parte reclamante y de cualquier usuario que visite la web en cuestión) en cualquier país en el que Google o cualquiera de sus subencargados de tratamiento de datos mantengan instalaciones, incluido los EE. UU., según declara la propia Google LLC en el documento de fecha de 9 de abril de 2021. Así, la actuación de Google LLC. se ciñe a lo estipulado y, por cuenta de FNMT, llevando a cabo el tratamiento de los datos personales necesarios para la correcta prestación del servicio.

En consecuencia, con independencia de que las SCCs (Google Ads y Medición: Cláusulas Contractuales Tipo (Módulo 3: Procesador a Procesador) vigentes en el momento de los hechos contemplaban en su Anexo I como exportador de datos a Google Irlanda, FNMT, como responsable del tratamiento, asume, junto con las demás condiciones de la contratación de los servicios de Google, los acuerdos relativos al tratamiento de datos y las SCCs que permiten que los datos sean transferidos a Google LLC, con sede en los Estados Unidos. Por lo tanto, FNMT es responsable de la transferencia internacional de datos que se produce como consecuencia del servicio prestado por Google LLC.

Con fecha 10 de julio de 2023 se aprobó por la Comisión la Decisión de Ejecución (UE) 2023/1795 relativa a la adecuación del nivel de protección de los datos personales en el Marco de Privacidad de Datos UE-EE. UU. con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, por lo que las transferencias internacionales que se realicen con posterioridad a la misma pueden quedar amparadas por la citada Decisión.

En la web ******URL.12*** puede comprobarse que Google LLC ha certificado su adhesión a los principios del Marco de Privacidad de Datos hasta el 13 de septiembre de 2024, debido a la necesidad de renovar anualmente dicha certificación. Por lo tanto, en la actualidad, las transferencias internacionales de datos a Google LLC en los EE. UU. están amparadas por el Marco de Privacidad de Datos UE. EE. UU.

Sin embargo, debe concluirse que, en la fecha en la que ocurrieron los hechos objeto de la reclamación, la FNMT no puede invocar ninguna de las herramientas previstas en el Capítulo V del RGPD para justificar las transferencias internacionales de datos personales de los visitantes a su sitio web, en particular identificadores únicos, direcciones IP, datos del navegador y metadatos, a Google LLC en los Estados Unidos, siendo de plena aplicación la doctrina establecida por el Tribunal de Justicia de la Unión Europea en la sentencia del caso Schrems II, por la que se invalidó la

decisión sobre el "EU-US Privacy Shield".

IV
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. (…)"

V
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".

No obstante, el artículo 77 "*Régimen aplicable a determinadas categorías de*

responsables o encargados del tratamiento" de la LOPDGDD establece un régimen específico aplicable en caso de infracciones cometidas por organismos públicos. Este artículo dispone lo siguiente:

"1*. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:*

(…)
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
(…)

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.
Cuando la competencia corresponda a una autoridad autonómica de protección de

datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

Este precepto establece que los procedimientos que tengan causa en infracciones en materia de protección de datos personales cometidas por las categorías de responsables o encargados del tratamiento enumerados en su apartado 1 se resolverán declarando la infracción.

Confirmado que la conducta efectuada por la FNMT constituye una vulneración del artículo 44 del RGPD, corresponde declarar que se ha cometido una infracción por parte de la FNMT.

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: DECLARAR que la **FABRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA**, con NIF Q2826004J, ha infringido lo dispuesto en el artículo 44 del RGPD, infracción tipificada en el Artículo 83.5 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a **FABRICA NACIONAL DE MONEDA Y TIMBRE-REAL CASA DE LA MONEDA**.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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.

1403-21112023

Mar España Martí
Directora de la Agencia Española de Protección de Datos