ECIJA
Av. Diagonal, 458, planta 8ª
08006 Barcelona · Tel: +34 933 808 255
www.ecija.com

Nota Informativa

Barcelona, 04 Marzo 2022

El uso de Google Analytics, ¿infringe la normativa?

Llevamos unos días donde los medios se han hecho eco de la importante cuestión acerca de ***"Google Analytics"***. Todo ello se debe al hecho de que, tanto la Autoridad de Control de Protección de Datos Austríaca (la DSB) como la Autoridad Francesa (la CNIL), se han pronunciado en contra del uso, tal y cómo se lleva a cabo, al menos, actualmente, de este tipo de **cookies**, utilizadas por gran cantidad de **páginas web** para ofrecer servicios más personalizados para el usuario. El motivo: su uso o instalación, podría no cumplir con lo dispuesto en el **RGDP** o **Reglamento Europeo de Protección de Datos** por suponer una **transferencia internacional de datos** que no cumpliría con las **medidas de seguridad** adecuadas, exigidas por la Unión Europea.

De este modo, **las resoluciones de las citadas autoridades podrían marcar una tendencia** o criterio para el resto de las **autoridades europeas** con competencia en la materia y, por ello, podríamos atrevernos a anticipar, en cierto modo, lo que podría suceder en el resto de los países. En nuestro país, no creemos que la **Agencia Española de Protección de Datos** tarde mucho en pronunciarse, pero nos parecía relevante empezar a tratar el asunto por su relevancia, mientras ello no sucede.

No obstante, para entender la problemática y el revuelo que esta situación está provocando, debemos entender primero, **qué es una cookie**; **qué tipo de cookies utiliza Google Analytics**, **qué es una transferencia internacional de datos,** y, por último, **por qué el uso de cookies de esta solución, supone una transferencia internacional de datos que, además, no cumpliría con las medidas de seguridad** exigidas en el citado RGPD.

En primer lugar, cabe decir (de forma muy simplificada) que una **cookie** es un archivo que se instala a través de una página web mientras el usuario la visita o navega por ella. Hay cookies que sirven para reconocer la ubicación del usuario, el idioma u otros aspectos más técnicos o funcionales y otras cookies que se utilizan para monitorizar lo que consultan los usuarios, a efectos de ofrecer un servicio más personalizado. Existen muchos otros matices y cuestiones, pero no es objeto de este documento extendernos en ello.

En segundo lugar, hay que indicar que **Google Analytics** utiliza este tipo de **cookies** o archivos que permiten monitorear el perfil de quién accede al sitio web, cuáles son las páginas más visitadas dentro de una página web, tasa de conversión, ubicación de los visitantes, entre otras funcionalidades.

En tercer lugar, una **transferencia internacional de datos**, a efectos de RGPD, significa compartir o enviar datos **fuera del espacio económico europeo**. Por lo tanto, no solo compartir o enviar datos a Estados Unidos sería una transferencia internacional de datos, sino que

también lo sería realizar un movimiento con datos identificativos o de personas a Sudamérica, Asia o África, por citar algunos territorios.

Por último, para **que una transferencia internacional de datos se considere segura** para Europa, el proveedor debe realizar el tratamiento de los datos en un país que tenga un sistema similar y esté validado por Europa, o que se produzcan otros escenarios de cumplimiento de medidas de seguridad, cosa que, según indican las autoridades austríaca y francesa, no sucede en el caso que nos ocupa.

No obstante, el problema principal, no es tanto en que se realice en sí la transferencia internacional de datos sino en el hecho de que en Estados Unidos existan unas leyes como la **FISA 702** o la **EO 12.333, que permiten que el gobierno de Estados Unidos** puede **rastrear e intervenir** estas **comunicaciones de datos** sin haber advertido de ello a los usuarios, sin consentimiento y no teniendo por qué ser legítimo este acceso a esta**.** Por lo tanto, la garantía de confidencialidad o **privacidad para el usuario**, podría quedar en entredicho.

¿De dónde proviene esta situación?

Todo proviene de que, en su momento, existió un pacto o acuerdo entre Estados Unidos y Europa que pretendía dar cobertura a esta situación y garantizar que los datos viajaran y se trataran de forma segura por parte de los proveedores estadounidenses.

Así, primero existió el acuerdo o protocolo conocido como **"Safe Harbor"** por el que las empresas estadounidenses que querían prestar servicios en Europa, se comprometían a cumplir unas medidas de seguridad y se adherían a dicho acuerdo o protocolo. No obstante, en 2015, este acuerdo fue declarado como no válido por el **Tribunal de Justicia de la Unión Europea (TJUE)**. A continuación, se promovió otro acuerdo, conocido como **"Privacy Shield"** pero este fue, nuevamente, declarado como inválido en julio de 2020, por el mismo tribunal.

Ambos acuerdos tenían la intención de garantizar que los datos que se comunicaban entre Europa y los Estados Unidos, se realizaban de manera lícita y cumpliendo determinadas medidas de seguridad. Pero entonces, en el escenario apareció el conocido activista y jurista **Max Schrems** quién provocó el cambio de las cosas.

Los casos Schrems I y Schrems II

Como decíamos, Max Schrems en su momento, inició una serie de acciones legales para impugnar el primer acuerdo, entendiendo que las prácticas de espionaje masivo de las agencias de inteligencia estadounidenses vulneraban los derechos fundamentales de los europeos. Esto ya se manifestó también en su momento por **Edward Snowden**, exempleado (y experto en seguridad informática) de la National Security Agency (NSA), hoy en el exilio.

Debido a esta primera acción, se dictó precisamente la conocida **Sentencia Schrems I** del TJUE donde se anuló el citado protocolo *Safe Harbor*, generando una situación de incertidumbre acerca de la posibilidad de seguir utilizando o no en Europa, los servicios de las grandes tecnológicas o *Big Tech* (como Google, Facebook, Microsoft, Apple, Amazon, etc.).

Derivado de esta situación, la Unión Europea y los Estados Unidos llegaron a un nuevo acuerdo, conocido como *Privacy Shield*, que pretendía convertirse en un nuevo marco

jurídico que aportaría una garantía estable y a largo plazo, que permitiría llevar a cabo las comunicaciones de datos entre Europa y Estados Unidos, de acuerdo con la ley.

Si bien, de nuevo, Max Schrems, impugnó este acuerdo puesto que las agencias de espionaje continuaban teniendo acceso a los datos y dejando, por lo tanto, indefenso al usuario. Ante ello, el TJUE optó por darle la razón, dictando la **Sentencia Schrems II** e invalidando el *Privacy Shield*.

El **caso Schrems II** provocó unos meses difíciles, en la que los distintos agentes económicos que querían seguir haciendo uso de las tecnológicas estadounidenses (la gran mayoría) debieron ajustar las transferencias de datos al resto de mecanismos previstos legalmente. Éstas incluían principalmente la revisión y confección de **cláusulas contractuales tipo (SCC)** y el diseño de **medidas técnicas y organizativas eficaces (las TOMs)**.

La implementación de las nuevas medidas no convenció a muchos, en particular, nuevamente, a Max Schrems quien, junto con la organización que preside, "*NOYB*", consideró (en sus propias palabras): "*en lugar de adaptar realmente los servicios para que cumplan con el RGPD* [Reglamento General de Protección de Datos Personales]*, las empresas estadounidenses han intentado simplemente añadir algún texto a sus políticas de privacidad y hacer caso omiso del Tribunal de Justicia. Muchas empresas de la UE han seguido el ejemplo, en lugar de optar por las opciones legales*".

La campaña "101 Dálmatas" y Google Analytics

Esta operación consistió en presentar **101 reclamaciones** por parte de NOYB ante las distintas autoridades de control de la UE, todo ello con el fin de hacer valer la sentencia **Schrems II**. En este caso, las reclamaciones tenían por objeto una operación muy concreta: *el* ***uso de las cookies de Google Analytics***. En particular, las quejas presentadas argumentaban que las empresas de la UE que hacían uso de estas *cookies* o herramientas de rastreo del usuario o visitante de una web en Internet, **no respetaban el fallo judicial del TJUE** ya que **el gobierno de Estados Unidos** podía seguir **rastreando e interviniendo estas comunicaciones quebrantando los derechos de los usuarios europeos.**

Debido a esta nueva reclamación, las autoridades de control ya se han empezado a manifestar, siendo la primera, la austríaca. Concretamente, la DSB ha considerado que Google **no ofrece garantías suficientes** de acuerdo con la normativa y el pronunciamiento establecido en el *caso Schrems II*. Se considera que el uso de las SCCs y las TOMs no son suficientes, si no se trata de medidas que efectivamente puedan salvaguardar los derechos de los europeos, **porque no son medidas "eficaces"** en la práctica. En la misma línea, se ha pronunciado la CNIL.

Estas decisiones tienen un impacto directo en casi todas las páginas web y entornos digitales de la Unión Europea. *Google Analytics* abarca un 70% de la cuota de mercado, siendo el programa de estadística más común. Es por ello por lo que **cabe preguntarse si en España, su uso, por parte de nuestra autoridad competente en la materia, también se considerará que infringe con la normativa.**

La Agencia Española de Protección de Datos (AEPD) no se ha pronunciado todavía, pero ya se encuentra investigando el caso. Si bien es cierto que su pronunciamiento podría ir en una

línea distinta a la de la DBS o la CNIL, la realidad es que las **autoridades de control han cooperado históricamente en la resolución de este tipo de casos**, y, si a ello le sumamos la evolución de los hechos vinculados a Schrems, y cuál ha sido la línea adoptada, podríamos esperar o **anticipar decisiones similares**, tanto **en España,** como en el resto de los países de la Unión Europea.

¿Qué debe hacer la empresa que está utilizando en Google Analytics en España?

Pues la situación no es fácil. Lo adecuado, sería analizar cada caso concreto y estudiar sus particularidades, pero, en general, la empresa podría elegir entre:

(1) Esperar a que la AEPD se pronuncie.
(2) Cesar en el uso de *Google Anlytics*.
(3) Buscar otro proveedor europeo que ofrezca tecnologías similares y que no realice transferencias de datos a los Estados Unidos.
(4) Esperar a que la Unión Europea y Estados Unidos fijen un nuevo acuerdo marco que permita que las transferencias de datos puedan realizarse de manera lícita, estable y sólida (lo que no parece probable que suceda, al menos, a corto plazo).
(5) Intentar adoptar medidas adicionales y solicitar el consentimiento de una manera muy transparente y concreta, pero, como hemos visto, esto no está siendo aceptado como válido, hasta el momento, por las autoridades que se han pronunciado siempre que estas medidas no resulten eficaces.

En conclusión, debemos ser prudentes y estar atentos al próximo pronunciamiento de la AEPD sobre el uso de *Google Analytics*, sin perjuicio de que, según las circunstancias concretas, resulte apropiado llevar a cabo un plan de prevención que permita encontrar soluciones o alternativas, a tiempo.

Recordemos, además que, en este caso, **quién incumpliría con la norma sería también el prestador de servicios o titular de una página web** puesto que es él quién utiliza estas herramientas de un tercero que no cumple.

En consecuencia, las empresas deben analizar esta situación como mínimo y, en base al propio **principio de proactividad** que establece el RGPD, adelantarse a posibles situaciones, buscando las soluciones más adecuadas, menos arriesgadas y garantistas para su negocio.

Así que, si tenéis cualquier duda o cuestión sobre este asunto y el planteamiento de posibles alternativas o soluciones, quedamos a vuestra disposición.

TMT, Protección de Datos & Compliance
+ 34 933 808 255
info.barcelona@ecija.com