INFORME

Google y Agencia Española de Protección de Datos: el caso de la implantación de soluciones digitales en la educación

Durante la pandemia de COVID-19, surgió la necesidad de convertir en virtuales y online los entornos de enseñanza. Muchas comunidades autónomas recurrieron a las soluciones ofrecidas por las grandes "Big Tech", en especial Google.

Pasada la crisis, sus servicios siguen implantados en muchos centros educativos, desde colegios a universidades. Estos paquetes tecnológicos han sido criticados en numerosas ocasiones. La principal razón es el acceso y tratamiento masivo de los datos que las corporaciones obtienen de ellas. Pero también la falta de claridad a la hora de otorgar los consentimientos, la dificultad de obtener información sobre los contratos que los usuarios (en su mayoría menores y sus familiares) están aceptando, o el poco control que tienen los centros educativos como responsables del tratamiento de datos.

Ya en 2021, la Agencia Española de Protección de Datos (AEPD) sancionó a la Consejería de Educación del Gobierno de Canarias por las infracciones de diferentes artículos del Reglamento General de Protección de Datos. No se respetaba el principio de "consentimiento informado" y se ponía en riesgo información de los alumnos amparada por dicho reglamento, así como la Ley Orgánica de Protección de Datos Personales.

En 2022, la Agencia sanciona de nuevo, por motivos similares, el uso obligatorio de dispositivos *Chromebook* de Google, implantados en un colegio de Vitoria. El dispositivo debía ser adquirido por cada familia, que lo recibían con las licencias de uso —de Google así como de diversas aplicaciones— instaladas de antemano. Su utilización implicaba la aceptación, sin posibilidad de revocarlos, de permisos que implicaban el acceso de la compañía a información tan sensible como la cámara, la ubicación, la cámara, los contactos, o el almacenamiento del dispositivo. La AEPD considera que no se había proporcionado a las familias información suficiente sobre los permisos, datos recogidos, y las figuras de "responsable" y "encargado" del tratamiento de los mismos.

En febrero de 2024, la AEPD responde a una consulta planteada por el Instituto Nacional de Tecnológicas Innovativas y Formación al Profesorado (INTEF) sobre la posibilidad de que se implemente en las aulas el uso de la *Solución tecnológica Workspace for Education*, desarrollada por Google Cloud EMEA Limited (Google en lo sucesivo).

La conclusión a la que llega la AEPD es que dicha implementación no es recomendable, basándose en los siguientes argumentos:

FALTA DE CLARIDAD EN LOS TÉRMINOS DE CONTRATACIÓN

En el paquete tecnológico de Google Workspace for Education se definen algunos servicios como **principales** y otros **adicionales**.

En los términos de contratación no se especifica en qué consiste cada uno de ellos, y es necesario acudir a documentos como las Condiciones de Privacidad relativas a Workspace. Ahí podemos comprobar que los servicios adicionales incluyen, entre otros, las búsquedas en Google, el uso de Google Maps o YouTube. Para estos servicios, se aplicarían las condiciones de uso generales para cualquier usuario de los mismos. Parece lógico pensar que estos servicios, presentados como adicionales, por tanto, no necesarios, sí lo serán. Una herramienta educativa basada en el ecosistema de Google donde no se pudiera hacer uso, por ejemplo, de las búsquedas de Google no tendría mucho sentido.

La AEPD destaca que el contratante en este caso los centros educativos, no deberían tener que acudir a *"a elementos de información externos para realizar una valoración de en qué medida va a ser necesario usar los servicios adicionales"*.

DATOS RECOPILADOS Y COMPARTIDOS POR GOOGLE

Según se establece en el Aviso de Privacidad de Google Workspace, incluirían, para el uso de los servicios principales:

- Todo lo que los usuarios envíen, almacenen, o reciban a través de los servicios principales.
- La información de la cuenta, nombre y correo electrónico.
- El contenido que el usuario vea, comparta, o aquel con el que interactúe (por ejemplo, dejando un comentario o un Me Gusta).
- La configuración de aplicaciones, navegadores y dispositivos. Incluyendo la red móvil, dirección IP, y actividad del sistema.
- Ubicación, determinada según la IP y el GPS.

Y para los servicios adicionales, además de lo anterior:

- Los términos de búsqueda, vídeos que ve, y aquellos con los que interactúa.
- Información de voz y audio cuando se utilice.
- Ubicación basada en IP, GPS, datos del sensor de su dispositivo e información sobre cosas cercanas a su dispositivo, como puntos de acceso Wi-Fi, torres de telefonía celular y dispositivos habilitados para Bluetooth.

En cuanto a los datos que se comparten, la AEPD resalta que, según la política de privacidad, Google podría compartir:

- Nombres de usuario, direcciones de correo electrónico y contraseñas.
- Direcciones de correo electrónico secundarias.
- Número de teléfono, fotos de perfil y cualquier información que el usuario añada a su cuenta.
- Información sobre cookies, donde se almacenan ajustes como el idioma de uso del servicio.

Cabe destacar que estos datos se compartirían con el administrador del servicio, que podría, por tanto, cambiar la contraseña de una cuenta y acceder a toda la información que haya en ella. Pero también con *afiliados y otros proveedores externos de Google*, así como en *cualquier país en el que Google o sus subencargados del tratamiento tengan instalaciones*.

FINALIDAD DEL TRATAMIENTO DE DATOS

La AEPD insiste en la poca claridad con la que se trata la finalidad del tratamiento de datos personales en las condiciones de contratación. Google menciona, sin especificar demasiado, que, para los **servicios principales**, las finalidades del tratamiento serán, con carácter general, *la prestación de los servicios, pero también existen otras finalidades adicionales como: mejorar los servicios; hacer recomendaciones para optimizar el uso de los servicios; proporcionar y mejorar otros servicios que solicite; dar apoyo; proteger a nuestros usuarios, clientes, el público y Google*.

En cuanto a las finalidades de los **productos adicionales**, destacan *brindar servicios personalizados, medida de rendimiento, y la muestra de anuncios en función de factores generales como las búsquedas realizadas, la hora del día o el contenido de una página que este siendo visualizada, así como la combinación de la información personal de un servicio con la que se recoja de otro*.

La respuesta de la AEPD destaca que hay finalidades que no sirven al propósito del "responsable" del tratamiento (el centro educativo), sino únicamente al "encargado" (Google). Además, están definidas en términos ambiguos e inconcretos (*mejorar servicios, dar apoyo, etc.*). Por otro lado, de otras finalidades se infiere que se producen a partir de la elaboración de perfiles, (*muestra de anuncios en función de factores generales*).

RESPONSABILIDAD A LA HORA DE OBTENER CONSENTIMIENTO

Según se detalla en los Términos del Servicio Google Workspace:

El Cliente es responsable de obtener los consentimientos y de proporcionar los avisos necesarios para permitir:

a) el uso y la recepción de los Servicios por parte del Cliente; y

b) el acceso, almacenamiento y tratamiento por parte de Google de los datos proporcionados por el Cliente (incluidos los Datos del Cliente) en virtud del Convenio.

Es decir, que recae sobre el usuario la obligación de que, a la hora de implementar GW, se haya otorgado el consentimiento tanto del cliente (que sería el Centro Educativo) como de los usuarios (que sería cualquier miembro de la comunidad educativa que fuera destinatario de la solución tecnológica, como el administrador, así como el profesorado y el alumnado).

La AEPD señala, además, que ese consentimiento no sería "libre e informado".

Si un alumno o alumna no aceptase dichos términos quedaría en condición de desigualdad al no poder hacer uso del servicio, por lo que no se puede hablar de libertad en el consentimiento.

Del mismo modo, las familias podrían no tener suficiente información para valorar la implicación de dicho consentimiento (sobre todo el almacenamiento, conservación y difusión). En ocasiones, incluso, se verían comprometidos los datos los de los demás miembros de la familia que utilicen dispositivos y la misma conexión que el menor usuario de una cuenta de Google Workspace.

MODIFICACIONES DEL SERVICIO

La AEPD informa de que, según los Términos del Servicio, Google podría hacer cambios "comercialmente razonables cuando lo estime oportuno", por lo que se deduce que, unilateralmente, podría modificar elementos que tienen incidencia en el tratamiento de datos personales. De este modo, se establece en una posición de toma de decisiones e impone contractualmente cláusulas que afectarían a dicho tratamiento, convirtiéndose así en el "responsable" del tratamiento de datos, y no solamente en el "encargado".

Además, Google establece que, en caso de contratar un nuevo subencargado de los datos durante la vigencia del contrato, avisaría a los usuarios con un margen de 30 días antes de que aquel empiece a prestar servicios. Los usuarios, por su parte, dispondrían de 90 días para rescindir el contrato ante esta nueva circunstancia. Esto supone que podría darse el caso en que la rescisión se produjera cuando ese subencargado ya dispone de la información personal de los usuarios. Cabe destacar que la rescisión del contrato por parte del Centro Educativo no supone una posibilidad real de negativa, sino una alternativa forzada por Google.

NORMATIVA

En la Adenda sobre tratamiento de datos, Google establece que una "Regulación de Protección de Datos No Europea también puede aplicarse al tratamiento de los Datos personales de los Clientes", y que esta Adenda "prevalecería independientemente de si la Regulación Europea de Protección de Datos [...] se aplica al tratamiento de los Datos personales de los Clientes".
La AEPD señala que esto no debería ser posible, en tanto que la Reglamentación de la UE sobre protección de datos es de obligado cumplimiento.

COMUNICACIÓN DE INCIDENCIAS

La AEPD destaca que, en sus términos, no existe un compromiso por parte de Google de notificar al responsable del tratamiento el incidente en menos de 72 horas como establece la normativa de la UE para violaciones de seguridad.

PROPORCIONALIDAD

Evaluando la necesidad de la plataforma de Google para cumplir con sus objetivos –que, en este caso, según la AEPD, serían los de la enseñanza relacionados con la adquisición de competencias digitales– frente a los riesgos que se asumen en el tratamiento de datos, se concluye que no superarían el juicio de proporcionalidad.

La adquisición de competencias digitales por los miembros de la comunidad educativa forma parte del derecho fundamental a la educación recogido en la Constitución Española, pero la necesidad de contratar servicios que se presentan como adicionales para alcanzar este fin pone en riesgo la privacidad de los menores.

Existiendo, en la mayoría de casos, otras alternativas para este fin, el riesgo de someter a tratamiento de información cuestiones como comportamientos psicológicos, culturales o educativos, convicciones religiosas, el rendimiento escolar y los intereses de los usuarios, entre otras, de nuevo exponen la privacidad a un peligro innecesario.

La AEPD destaca que, la recogida invasiva de información personal, la posibilidad de usarla para elaborar perfiles y el hecho de que esta información pueda transferirse a terceros son un riesgo innecesario. Se trataría de una recogida masiva de datos, que implica un gran número de afectados, muchos de ellos menores de edad.


AETD
Asociación Europea
para la Transición Digital