avances en Supervisión educativa
Revista de la Asociación de Inspectores de Educación de España

Plataformas para el aprendizaje en línea: La protección de datos en el ámbito educativo

/

E-learning platform: Data protection in the educational scope

José Manuel Cabrera Delgado

Inspector de Educación de la Comunidad Autónoma de Canarias

DOI

https://doi.org/10.23824/ase.v0i33.680

Resumen

La suspensión de la actividad docente presencial, derivada de la crisis sanitaria ocasionada por la COVID-19, ha tenido como consecuencia directa que las distintas Administraciones educativas dirijan su mirada hacia la enseñanza a distancia. Principalmente, por la posibilidad de permitir compatibilizar la prevención de la enfermedad con mantener una relación interpersonal con el alumnado lo más cercana posible. En este contexto, la utilización de distintas plataformas educativas se ha vuelto imprescindible y con ello la necesidad de trabajar con datos personales de todos los intervinientes en el proceso, convirtiendo la seguridad y protección de los datos en una preocupación de instituciones y gobiernos que debe ser gestionada desde todos los ámbitos.

El presente artículo tiene como finalidad hacer visible algunos de los aspectos más complejos y relevantes en el tratamiento de datos personales por parte de las plataformas para el aprendizaje en línea, así como determinar aquellas actuaciones de la Administración o de los centros educativos que se deben seguir para una mejor protección de los usuarios, de conformidad con los derechos y obligaciones que

impone la normativa vigente. Para ello, y a modo de ejemplificación, se analizan dos de las plataformas más ampliamente utilizadas por el profesorado y alumnado español: *G Suite for Education* y *Microsoft 365 Education.*

Palabras clave: plataforma educativa; enseñanza a distancia; protección de datos; privacidad; G Suite for Education; Microsoft 365 Education.

Abstract:

The suspension of face-to-face teaching activity, derived from the health crisis caused by COVID-19, had as a direct consequence that the different educational Administrations turned their eyes towards distance learning. Mainly, due to the possibility of making the prevention of the disease compatible with maintaining an interpersonal relationship with the students as closely as possible. In this context, the use of different educational platforms has become essential and with it the need to work with personal data of all those involved in the process, making the security and protection of data a concern of institutions and governments that should be managed from all ambits involved.

The purpose of this article is to make visible some of the most complex and relevant aspects in the treatment of personal data by online learning platforms, as well as to determine those actions by the Administration or educational centers that must be followed for better protection of users, in accordance with the rights and obligations imposed by current regulations. For this, and as an example, two of the platforms most widely used by Spanish teachers and students are analyzed: G Suite for Education and Microsoft 365 Education.

Key words: educational platform; e-learning; Data Protection; Privacy; G Suite for Education; Microsoft 365 Education.

1. Introducción

La adecuación del modelo de enseñanza y aprendizaje que ha tenido que afrontar la educación en nuestro país, desde el comienzo de la crisis sanitaria originada por la COVID-19, transformando un modelo educativo predominantemente presencial en un modelo de enseñanza a distancia, sin apenas tiempo y sin la formación deseable, preveía, desde un principio, la aparición de dificultades que iban a afectar a la sociedad en general y a muchas familias en particular, no solo en cuanto a los aspectos tecnológicos y escasez de medios (brecha digital), sino también en cuanto a los económicos y sociales (brecha educativa).

A pesar de estas dificultades fue el profesorado el primero y mayor partícipe en liderar el cambio que la situación exigía, buscando múltiples alternativas y convirtiendo la enseñanza en línea en un elemento esencial que permitiera una nueva interacción entre el profesorado y su alumnado, alejando la tradicional consideración del aula como el espacio físico natural y los horarios escolares como el habitual espacio temporal.

Una vez que la situación actual deja entrever el regreso al modelo de enseñanza presencial, en el firme convencimiento de que la enseñanza a distancia vino para quedarse, por ser un complemento significativo que proporciona al alumnado un amplio margen de autonomía en la planificación de sus estudios y en el avance de su desarrollo personal, se hace imprescindible conciliar la seguridad y privacidad de los datos personales que son necesarios para su gestión a través de las plataformas educativas que la hacen posible.

Pues es obvio, que hoy en día se ponen a disposición de la ciudadanía en Internet multitud de servicios y aplicaciones que con diferentes propósitos nos solicitan nuestros datos personales para su gestión. Esta sobreexposición de datos, que se ha visto incrementada a su vez por el uso masivo del teléfono móvil, ha conllevado la necesidad de la creación de un marco regulatorio jurídico que proteja las libertades y derechos fundamentales de las personas y, en particular, de su intimidad. Ese marco jurídico, que se ha ido desarrollando en los últimos veinticinco años en la Unión Europea, ha determinado que las aplicaciones y plataformas proporcionadas por instituciones y empresas, públicas y privadas, que hacen uso de la red para facilitar

la interconexión, hayan tenido que adaptarse a los requisitos y exigencias determinadas en su articulado.

En base a lo anterior, resulta imprescindible conocer para la Administración educativa o titulares de centros privados, responsables del tratamiento de los datos personales, el marco jurídico que regula el funcionamiento de las plataformas educativas para el aprendizaje puestas a disposición del alumnado y profesorado, así como los derechos y deberes que en su cumplimento deben afrontar.

2. Marco jurídico de la protección de datos

El marco jurídico actual de protección de datos personales en la Unión Europea lo conforman el **Reglamento de la Unión Europea (UE) 2016/679,** relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[1] (en adelante RGPD), y con respecto a nuestro país la **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[2] (en adelante, LOPDGDD), ley que desarrolla el citado Reglamento.

El RGPD entró en vigor el 24 de mayo de 2016 y es de aplicación directa desde el 25 de mayo de 2018, por su parte la LOPDGDD entró en vigor el 7 de diciembre de 2018.

El RGPD plantea diferentes novedades con respecto a la normativa anterior, destacando las siguientes:

- Nuevos derechos con respecto a los interesados. Además de los conocidos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) se añaden derechos como la transparencia a la información, el derecho al olvido, derecho de limitación del plazo (los datos personales deben ser destruidos una vez que se haya cumplido la finalidad para la cual se hubiesen obtenido) y derecho a la portabilidad (transmisión de datos entre un responsable y otro) (art. 13, RGPD).

[1] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[2] https://www.boe.es/eli/es/lo/2018/12/05/3/con

- Se amplía el deber de información añadiendo la necesidad de informar sobre la base legal para el tratamiento de los datos, el periodo de conservación, la posibilidad de hacer reclamaciones, los derechos de que disponen los titulares (art. 14, RGPD).
- El consentimiento requiere de una declaración del interesado o una acción positiva que manifieste su conformidad (art. 22, RGPD). Deja de ser suficiente la inacción o las casillas en blanco. De igual forma, se establece como edad mínima para el consentimiento con respecto a los servicios de información la edad de 16 años o la edad que establezca una ley nacional que no podrá ser inferior a 13 años (art. 8, RGPD). España establece como edad mínima los 14 años.
- Creación del registro de actividades de tratamiento, registro interno obligatorio para organizaciones con más de 250 empleados, o que realicen tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados o que incluya categorías especiales de datos o datos relativos a condenas e infracciones penales (art. 30, RGPD). Desaparece la necesidad de notificar y registrar los ficheros de datos ante la Agencia Española de Protección de Datos.
- Exigencia de una responsabilidad proactiva para el responsable del tratamiento. Debe establecer las medidas técnicas y organizativas adecuadas (art. 32, RGPD).
- Creación de la figura del Delegado de Protección de Datos que será obligatorio para organismos e instituciones públicas, empresas que superen los 250 empleados, empresas cuya actividad sea el tratamiento de datos, entidades o empresas que manejen datos especialmente protegidos. El Delegado de Protección de Datos tendrá como finalidad principal garantizar el correcto tratamiento de los datos en la entidad, empresa, organismo o institución de la que dependa (art. 37 y ss., RGPD).

Por su parte la LOPDGDD concretó diversos aspectos a la vez que introdujo los siguientes cambios y novedades principales:

- Con respecto al consentimiento de los menores, se determina que el tratamiento de los datos personales de un menor de edad únicamente podrá

fundarse en su consentimiento, cuando sea mayor de catorce años (art. 7, LOPDGDD).

- Con respecto a la información, se establece la posibilidad de proporcionar al interesado información básica sobre el tratamiento de datos e indicarle una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información (art. 11, LOPDGDD).
- Se establece la licitud de ciertos tratamientos de datos. Por ejemplo, los tratamientos con fines de vigilancia que deberán realizarse con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones siguiendo las condiciones establecidas (art. 22, LOPDGDD).
- Con respecto al delegado de protección de datos se enumeran entidades que en todo caso deberán designarlo, entre ellas, los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas (art. 34, LOPDGDD).
- Se establece un sistema de sanciones o actuaciones correctivas para determinadas conductas, estableciendo distinción entre infracciones muy graves, graves y leves, siguiendo la diferenciación del RGPD según cuantía.

3. G Suite for Education y Office 365 Education

G Suite for Education y *Office 365 Education* se han convertido en dos de las plataformas educativas para el aprendizaje en línea más utilizadas por el alumnado y profesorado españoles.

- G Suite for Education es la solución que Google proporciona, específicamente, para los centros educativos y contiene dos categorías de servicios. Unos servicios principales constituidos por aplicaciones web como *Gmail*, *Drive*, *Calendar*, *Classroom*, *Forms*, *Sites*, etc., y unos servicios adicionales como *Youtube*, *Maps* o *Blogger* que se pueden utilizar de forma opcional si el centro educativo lo considera.

La difusión y auge de *G Suite for Education* se debe a las posibilidades que proporciona para el trabajo con el alumnado y, en concreto, a la popularidad de la aplicación denominada ***Classroom*** que permite a los docentes asignar actividades,

comunicarse con su alumnado, realizar seguimiento de sus tareas, enviar vídeos, audios, simulaciones, etc.

Según G Suite for Education (2020) la plataforma permite configurar un sistema de correo electrónico para todo el centro educativo utilizando Gmail, a la vez, que posibilita al alumnado tener una capacidad de espacio en *Drive* para almacenar documentos, imágenes, videos, etc. De igual forma permite la utilización de diversos servicios como *Calendar* (calendario), *Docs* (procesador de texto), *Sheets* (hoja de cálculo), *Slides* (presentaciones), *Forms* (cuestionarios), *Meet* (videollamadas).

- *Office 365 Education* es el nombre que recibe la solución gratuita que proporciona Microsoft a los centros educativos para su utilización como plataforma para el aprendizaje en línea.

Office 365 Education (2020) posibilita el uso a los estudiantes y profesorado de sus aplicaciones más conocidas (*Word, Excel, PowerPoint, OneNote*) otorgándoles un espacio de almacenamiento y un correo electrónico, todo ello a través de servicios en la nube. Además de lo anterior, proporciona ***Microsoft Teams*** que al igual que *Classroom* se ha consolidado como la herramienta más utilizada para el trabajo docente, permitiendo al profesorado crear grupos con el alumnado (equipos) con los cuales poder comunicarse fácilmente, compartir archivos, asignar tareas, emitir calificaciones, en definitiva, colaborar de forma remota.

Las dos plataformas almacenan los datos suministrados en una red de servidores remota accesible a través de internet, recibiendo el nombre de servicios de computación en la nube. Característica que ha venido a suscitar reticencias en relación con la legislación europea de protección de datos y con su seguridad.

4. Tratamiento y protección de los datos por parte de G Suite for Education

Los centros educativos que quieren utilizar *G Suite for Education* deben establecer un contrato de prestación de servicios (Acuerdo de G Suite for Education (2020)[3]) entre el centro educativo y la empresa *Google Ireland Limited*, empresa constituida de conformidad con la legislación irlandesa, con sede en Dublín, y que en Europa es la empresa que gestiona todos sus servicios.

[3] https://gsuite.google.com/terms/education_terms.html

Es parte sustancial de ese contrato la Adenda de Tratamiento de Datos (2020)[4] que establece los derechos y obligaciones de las partes en relación con el tratamiento y seguridad de los datos.

De ambos documentos se extraen las siguientes consideraciones como relevantes:

- A los datos personales suministrados por los centros educativos les será de aplicación la normativa europea de protección de datos. También, podrá ser aplicable la normativa de protección de datos de países externos a la Unión Europea.
- Google no procesará los datos personales suministrados por los centros con fines publicitarios ni emitirá publicidad en los servicios ofertados.
- Productos adicionales puestos a disposición de los centros educativos por Google, si los centros optan por instalarlos, sí podrán acceder a los datos suministrados en caso de que fuera necesario.
- La eliminación de datos será responsabilidad del centro educativo. En relación con las copias de seguridad, una vez solicitada la completa eliminación de los datos por parte de los centros, Google cumplirá con estas instrucciones tan pronto como sea razonablemente posible y dentro de un período máximo de 180 días, a menos que las leyes europeas o nacionales requieran un almacenamiento superior.
- Es responsabilidad de Google implementar y mantener las medidas técnicas y organizativas para proteger los datos de los centros educativos contra la destrucción, pérdida, alteración, divulgación o acceso no autorizados o ilegales.
- Google notificará a los centros educativos con prontitud y sin demora indebida cualquier incidente relacionado con los datos suministrados, y tomará las medidas razonables para minimizar el daño y proteger los datos.
- Es responsabilidad de la Administración o de los titulares de los centros privados, como responsables del tratamiento, el uso adecuado de los servicios y del almacenamiento de copias de datos.

[4] https://gsuite.google.com/intl/es/terms/dpa_terms.html

- Google puede almacenar y procesar los datos de los centros educativos en cualquier lugar donde Google mantenga instalaciones.
- En relación con los derechos de propiedad intelectual e industrial los centros educativos y sus usuarios son considerados los titulares de todos ellos.

En relación con los centros educativos, procede detenerse en dos cuestiones que han suscitado recurrentes dudas: la transferencia de datos fuera de los límites de la Unión Europea y la cesión y consentimiento por parte de los interesados.

4.1. Transferencia de datos fuera de los límites de la Unión Europea

Google hace uso de dos posibilidades establecidas en el RGPD para las transferencias de datos fuera de la Unión Europea en su servicio *G Suite*: las transferencias basadas en una decisión de adecuación (art. 45, RGPD) y las transferencias mediante garantías adecuadas (art. 46, RGPD).

Con respecto a las transferencias basadas en una decisión adecuada, corresponde a la Comisión Europea determinar que los destinatarios de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional con nivel de protección adecuado. Para el caso de Estados Unidos hay que hacer referencia a la Decisión (UE) 2016/1250[5] de la Comisión, por la que los Estados Unidos garantiza un nivel adecuado de protección en el marco del Escudo de la Privacidad UE-EE. UU.

El Escudo de la privacidad UE-EE. UU.[6] es un acuerdo político entre la Comisión Europea y el gobierno de los Estados Unidos que ofrece mecanismos de control y seguridad, incluyendo limitaciones que eviten el acceso generalizado a los datos por parte de las autoridades. Las empresas que forman parte del Escudo de la Privacidad pueden ser consultadas en la página https://www.privacyshield.gov/list.

Google cumple con el Escudo de la Privacidad UE-EE. UU. y, por tanto, de acuerdo con el Reglamento, no es necesario ninguna otra autorización para realizar transferencias de datos personales que tengan como destino los Estados Unidos.

[5] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016D1250&from=es

[6] https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf

Con respecto a transferencias mediante garantías adecuadas que doten a los usuarios de derechos y acciones legales efectivas, *G Suite for Education* hace uso de cláusulas contractuales previstas en su contrato de servicios, y Adenda consiguiente, posibilitando que los datos personales puedan ser transferidos no solamente a países que hayan sido declarados con nivel adecuado de protección por la Comisión Europea, sino también a terceros países que no cuenten con la citada declaración.

4.2. Cesión y consentimiento por parte de los interesados

El RGPD define el tratamiento de los datos como: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*" (art. 4, RGPD).

De igual forma, determina como responsable de ese tratamiento a la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, y como encargado del tratamiento a la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable (art. 4, RGPD).

Con respecto a *G Suite for Education*, de acuerdo con lo anterior, son responsables del tratamiento cuando se trate de centros públicos normalmente la Administración educativa, es decir, la Consejería de la Comunidad Autónoma competente en materia educativa, y cuando se trate de centros concertados o privados lo serán los propios centros educativos (Agencia Española de Protección de Datos, 2018, p.12). Por su parte, el encargado del tratamiento es la empresa *Google Ireland Limited*[7] y no las personas físicas que tengan acceso a los datos personales en su condición de empleados del centro o de la Administración educativa (Agencia Española de Protección de Datos, 2018, p.13). Por tanto, el equipo directivo del centro, los

7 El RGPD y, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establecen distintas obligaciones para los responsables y encargados del tratamiento.

profesores, o el personal de administración y servicios del centro educativo no son encargados del tratamiento.

Esta aclaración es oportuna porque a partir de ella debemos establecer si existe o no cesión de datos por parte del centro educativo cuando se utiliza *G Suite for Education*.

El Tratamiento de datos será lícito si se cumple al menos una de las siguientes condiciones (art. 6, RGPD):

- el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.
- el tratamiento es necesario para la ejecución de un contrato…
- el tratamiento es necesario para el cumplimiento de una obligación legal…
- el tratamiento es necesario para proteger intereses vitales…
- el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos…

Respecto a los centros educativos, su licitud se encuentra amparada en el cumplimiento de una obligación legal, como determina la Ley Orgánica 2/2006, de 3 de mayo, de Educación[8] en su Disposición adicional vigesimotercera apartado primero: "*Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos*".

Una vez aclarado lo anterior, la pregunta que se plantea de forma inevitable es si existe cesión de datos. Y la respuesta a la misma se obtiene al diferenciar quién actúa como responsable y quién como encargado del tratamiento. Como la Agencia Española de Protección de Datos (en adelante, AEPD) ha indicado en múltiples resoluciones, la figura del encargado del tratamiento es una respuesta a la necesidad de externalizar servicios que puedan ser realizados por un tercero de

[8] https://www.boe.es/buscar/act.php?id=BOE-A-2006-7899

forma más eficiente. Es por lo que, si el acceso a los datos tiene como única finalidad la de proporcionar el servicio, realizándose en nombre y por cuenta del responsable, no podemos hablar de estar ante una cesión de datos. Exigiéndose para que no exista cesión, de acuerdo con el artículo 28.3 del RGPD, la existencia de "*un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable"*.

En ese sentido, el Acuerdo de G Suite for Education (2020) y la correspondiente Adenda de Tratamiento de Datos (2020) establecido entre *Google Ireland Limited* y la Administración o los titulares de los centros privados, confirman el cumplimiento de las condiciones que determinan que Google actúa como encargado del tratamiento de datos. Eso sí, para los servicios principales que proporciona *G Suite for Education* y no para otros servicios adicionales que pueda prestar y que deberán ser contratados, si así fueran necesarios. Con respecto a estos servicios adicionales, el responsable del tratamiento asume otros derechos y obligaciones y, por tanto, también la responsabilidad que pudiera derivarse del uso de estos servicios. Entre otros servicios: *Youtube*, *Maps* o *Blogger*.

En base a lo anterior, la necesidad del consentimiento por parte de los usuarios partirá de diferenciar los servicios principales suministrados por *G Suite for Education* de otros servicios adicionales, pues en los primeros ha quedado patente que *Google Ireland Limited* actúa específicamente como encargado del tratamiento, no siendo responsable de su uso y finalidad.

Por tanto, con respecto a los servicios principales suministrados por *G Suite for Education* no sería necesario obtener el consentimiento, pues la Administración o los centros educativos actúan como responsables y el tratamiento es necesario para el cumplimiento de una obligación legal, en el ejercicio de la función educativa (Ley Orgánica 2/2006, de 3 de mayo, de Educación, DA 23ª). Lo cual no es óbice para que el responsable cumpla con sus obligaciones, en especial, las referentes a la transparencia e información establecidas en el artículo 11 del RGPD:

- Identidad del responsable del tratamiento y de su representante, en su caso.

- Finalidad del tratamiento.
- Posibilidad de ejercer los distintos derechos.

Caso distinto es el que hace referencia a posibles servicios adicionales que pudieran ser contratados. En ellos sí se hace necesario obtener el consentimiento de los interesados entendiéndose como tal: "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*" (art. 4.11 RGPD y art. 6 LOPDGDD).

Consentimiento que el alumnado mayor de 14 años podrá realizar por sí mismo, no siendo necesario la confirmación del titular de la patria potestad o tutela del menor (art. 7, LOPDGDD).

5. Tratamiento y protección de los datos por parte de Office 365 Education

Microsoft presta el servicio de *Office 365 Education* a través de *Microsoft Ireland Operations Limited*, filial establecida en Irlanda, a través del correspondiente contrato de servicios[9] que incluye una Adenda con respecto a la Protección de Datos[10].

De acuerdo con la Adenda de Protección de datos de servicios online de Microsoft (2020), en relación con los datos suministrados por centros educativos situados en la Unión Europea, se extraen los siguientes derechos y obligaciones como relevantes:

- Microsoft cumplirá todas las leyes y reglamentos aplicables en su prestación de servicios online, incluyendo cualquier ley aplicable en materia de notificación de violaciones de la seguridad y requisitos de protección de datos.
- Los centros educativos deben cumplir con todas las leyes y reglamentos correspondientes al uso de los servicios online, incluidas las leyes relacionadas con la privacidad, datos biométricos, confidencialidad de las comunicaciones y requisitos de protección de datos

[9] https://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=Spanish

[10] https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=16059

- Microsoft no utilizará ni procesará los datos de los centros educativos para: (a) generar perfiles de usuarios, (b) publicidad o fines comerciales similares, o (c) investigación de mercado que apunta a crear nuevas funcionalidades, servicios o productos, o para cualquier otro propósito, salvo que dicho uso o procesamiento se realice de acuerdo con las instrucciones documentadas del cliente.
- En todo momento durante el periodo de vigencia de su suscripción, los centros educativos tendrán la capacidad de acceder a los datos almacenados en cada Servicio Online, así como tendrá también la capacidad de extraerlos y eliminarlos.
- Microsoft conservará los datos que sigan almacenados en los Servicios Online en una cuenta con funcionalidad limitada durante los noventa (90) días siguientes a la expiración o terminación de la suscripción, de tal modo que los centros educativos puedan extraer los datos. Después del término del período de retención de noventa (90) días, Microsoft desactivará la cuenta y eliminará los datos dentro de un período de noventa (90) días adicionales, salvo que la legislación aplicable permita o solicite a Microsoft, o que se autorice, retener esos datos.
- Microsoft implementará y mantendrá las medidas técnicas y organizativas apropiadas para proteger los datos de cualquier destrucción, pérdida, alteración, revelación autorizada o acceso accidental o ilegítimo.
- Los datos que Microsoft procesa en nombre del centro educativo se pueden transmitir, almacenar y procesar en Estados Unidos o en cualquier otro país en que Microsoft u otro procesador externo contratado por el mismo tenga operaciones. Todas las transmisiones fuera de la Unión Europea se regirán por cláusulas contractuales.
- Los centros educativos conservan todos los derechos, la titularidad y los intereses sobre los datos no adquiriendo Microsoft derechos sobre ellos.

5.1. Transferencia de datos fuera de los límites de la Unión Europea

Microsoft, en el ámbito de la Unión Europea, utiliza los mismos mecanismos para *Microsoft 365* que Google para *G Suite*. Es decir, la transferencia de datos a un

tercer país cuando la Comisión haya determinado que ese tercer país garantiza un nivel adecuado de protección (art. 45, RGPD) y las transferencias realizadas con garantías adecuadas donde los interesados cuenten con derechos exigibles y acciones legales efectivas (art. 46, RGPD).

Con respecto a las transferencias basadas en una decisión adecuada (art. 45, RGPD), *Microsoft 365* está incluido dentro del Escudo de la privacidad UE-EE. UU. y cumple con los requisitos que rigen el uso y el tratamiento de datos personales transmitidos desde la Unión Europea, así como el acceso y los mecanismos para la resolución de litigios que las empresas participantes deben proporcionar a sus ciudadanos[11]. Este es el mecanismo utilizado cuando los datos personales se transfieren desde la Unión Europea a los Estados Unidos mediante servicios en línea no básicos.

Por el contrario, cuando se hace uso de servicios en línea básicos la transferencia está sujeta a los compromisos de Microsoft y sus cláusulas contractuales. Es decir, a las transferencias realizadas con garantías adecuadas (art. 46, RGPD). Cláusulas presentes en el contrato de servicios y acuerdo suplementario proporcionado por Microsoft a sus clientes[12].

Las cláusulas y contratos fueron estudiados por la AEPD, cuando todavía era requisito necesario su autorización, resolviendo adecuadas las garantías establecidas para la transferencia internacional de datos con destino a los Estados Unidos[13].

5.2. Cesión y consentimiento por parte de los interesados

Como determinan los términos del servicio contratado y la Adenda de *Office 365 Education,* la Administración o los titulares de los centros privados, tienen la responsabilidad del tratamiento de datos siendo *Microsoft Ireland Operations Limited* el encargado de realizar el procesamiento.

[11] Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, por la que los Estados Unidos garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016D1250&from=es

[12] De conformidad con la Decisión 2010/87/UE de la Comisión Europea, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países.

[13] Resolución Nº Expediente: TI/00032/2014, de 9 de mayo de 2014.

Tratamiento de datos que es lícito en base al cumplimiento de una obligación legal, según Disposición adicional vigesimotercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

El contrato de servicios de *Office 365 Education* es claro al determinar que no existe cesión de datos al actuar Microsoft realizando solamente funciones de gestión. Debiendo cumplir el responsable con las obligaciones que establece el RGPD, en especial, la de información a los usuarios y elegir un encargado que ofrezca garantías de seguridad y protección de los datos personales.

Con respecto al consentimiento, *Office 365 Education* no hace distinción entre servicios esenciales o adicionales como realiza *G Suite for Education*. Los servicios que proporciona están dentro del marco establecido de los términos del servicio contratado y de la Adenda de protección de datos, actuando Microsoft exclusivamente como encargado y no teniendo ninguna responsabilidad en el uso o finalidad de los datos suministrados. No siendo necesario solicitar consentimiento a los usuarios, al actuar *Office 365 Education* como plataforma en la cual la Administración o los titulares de los centros privados actúan como responsables en el ejercicio de la función educativa. Sin olvidar que eso no es óbice para cumplir con las obligaciones de transparencia e información establecidas en el RGPD.

6. Obligaciones por parte de la Administración o los titulares de los centros privados en el uso de las plataformas

La Administración o los titulares de los centros privados, en ambas plataformas, desempeñan el papel de responsables en el tratamiento de los datos personales. El RGPD determina para los responsables numerosas, complejas y distintas obligaciones a cumplir que se ven facilitadas a través de la posibilidad de designar encargados para su tratamiento que, en lo que respecta a este artículo, lo desempeñan las filiales de Google y Microsoft situadas en Irlanda.

El RGPD impone al responsable a la hora de designar los encargados la siguiente obligación: "*Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que*

el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado" (art. 28, RGPD).

Es por tanto que la asignación de encargado del tratamiento tiene como objeto ayudar al responsable a garantizar el cumplimiento de las distintas obligaciones siguiendo las indicaciones de este último. Para ello tanto *G Suite for Education* como *Office 365 Education* permite la asignación de usuarios administradores que, mediante el uso de consolas específicas de administración, puedan tomar decisiones con respecto a la gestión y seguridad de los datos del alumnado y profesorado usuario.

Con respecto a las obligaciones propias del responsable, no delegadas en el encargado del tratamiento, la Administración o los titulares de los centros privados deberán adoptar decisiones en los siguientes ámbitos:

- **Transparencia e información a los usuarios**: es una obligación propia de los responsables pues son ellos los que personalizan los servicios a realizar por el encargado del tratamiento. Dicha información debe incluir información básica (identidad del responsable del tratamiento, finalidad del tratamiento, derechos ejercitables), así como una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información, entre ella, los términos del servicio contratado y las respectivas Adendas sobre privacidad y protección de datos personales. En caso de hacer uso de servicios adicionales, la Administración o los titulares del centro privado deberán proporcionar información sobre las características de estos servicios y en caso de ser necesario solicitar el respectivo consentimiento para su uso. Siendo de gran importancia que se comunique esta información de manera clara y concisa, con un lenguaje sencillo que permita su entendimiento, más aún cuando esta información puede ir dirigida a menores de edad.

- **Consentimiento**: determina el RGPD que el tratamiento de datos será lícito cuando los datos personales sean tratados con el consentimiento de los interesados o sobre alguna otra base legítima establecida conforme a Derecho. Con respecto a las dos plataformas educativas, esa base legítima es la obligación legal, determinada en la Ley Orgánica de Educación, que permite a los centros educativos recabar los datos personales de su alumnado cuando sean necesarios para el

ejercicio de la función educativa. Función educativa que cumplen los responsables a través de las plataformas educativas analizadas que actúan gestionando distintos servicios, al amparo de un contrato y respectivas adendas donde la protección de datos cumple con la normativa europea. Es por ello que los responsables, la Administración o los titulares del centro privado, una vez decidida la conveniencia de utilizar estas plataformas en sus órganos de gobierno, no estarán obligados a requerir el consentimiento al alumnado. Ahora bien, las plataformas educativas en su evolución han ido incorporando otros nuevos servicios o aplicaciones, incluso de otras empresas, que conllevaría tratamientos de datos con finalidades distintas y que sí requieren el consentimiento del alumnado y del profesorado. Siendo obligación de los responsables requerir para su uso el consentimiento que, para ser válido, debe consistir en un acto afirmativo expreso que refleje una manifestación de voluntad libre, específica, informada e inequívoca. No sirviendo para ello, consentimientos genéricos ni aquellos que ofrezcan información incompleta sobre la gestión que realizan de la protección de datos de los usuarios. A este respecto, debemos recordar que la ley española determina que el tratamiento de los datos personales de un menor de edad, únicamente, podrá fundarse en su consentimiento cuando sea mayor de catorce años.

- **Extensión del tratamiento y plazo de conservación**: las dos plataformas permiten a los responsables establecer la extensión de la duración de los servicios prestados, así como el correspondiente borrado de forma consistente de los datos suministrados. De tal forma que, una vez finalizado el servicio prestado, las plataformas realizarán la eliminación de los datos y copias de seguridad en un plazo de tiempo razonable (en ambos casos no superior a 180 días), salvo que la legislación aplicable impida devolver o destruir la totalidad o una parte de los datos personales transmitidos. El RGPD es claro al establecer como responsabilidad de la Administración o de los titulares de los centros privados el garantizar que los datos personales no se conservan más allá del tiempo necesario, estableciendo plazos para su supresión o revisión periódica. En tal sentido, las copias de seguridad de datos extraídos de la plataforma deben ser eliminadas de igual forma.

- **Pertinencia y minimización de los datos**: es un principio básico relativo al tratamiento de datos personales que los datos recabados sean adecuados,

pertinentes y limitados a lo necesario en relación con el fin para el cual son solicitados. Principio que se convierte en una responsabilidad para la Administración o los titulares de los centros privados dentro de la más amplia de vigilancia, control y cuidado que se debe acometer en el uso de las plataformas. Para ello resulta de vital importancia la designación de usuarios administradores que realicen funciones como las de gestionar perfiles de usuarios y asignar permisos de lectura de los datos, impidiendo un acceso general por parte del alumnado y del profesorado, así como la posibilidad de que terceras personas puedan acceder a ellos. De igual forma, se hace necesario extremar la precaución sobre los datos solicitados, en particular para evitar el tratamiento de datos sensibles no necesarios en el ejercicio de la función educativa.

- **Registro de las actividades del tratamiento**: la Administración o los titulares de los centros privados deberán elaborar un registro de las actividades de tratamiento de datos efectuadas bajo su responsabilidad (art. 30, RGPD). Obligación nueva que suprime la obligación anterior de notificar la creación de ficheros a la AEPD e inscribirlo en el Registro General de Protección de Datos. El registro de las actividades de tratamiento es un registro interno que debe constar por escrito y que podrá ser solicitado por la AEPD. El registro como indica la Autoridad Catalana de Protección de Datos (2018): “se puede organizar en torno a operaciones de tratamiento concretas, vinculadas a una finalidad básica común de todas ellas (por ejemplo, gestión académica o gestión de recursos humanos y nóminas), o bien de acuerdo con otros criterios” (p.19). A este respecto, tanto la AEPD como la Autoridad Catalana de Protección de Datos han desarrollado aplicaciones que a modo de ejemplo facilitan la creación del registro de las actividades de tratamiento[14]. El registro deberá contener la información establecida en el artículo 30.1 del RGPD que a modo de exposición se concreta en:

a) nombre y los datos de contacto del responsable y del delegado de protección de datos;
b) los fines del tratamiento;

[14] Autoridad Catalana de Protección de datos. Aplicación para gestionar el registro de las actividades de tratamiento. https://apdcat.gencat.cat/es/documentacio/RGPD/altres_documents_dinteres/Aplicacio-per-gestionar-el-registre-de-les-activitats-de-tractament/index.html

c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de los destinatarios;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

- **Análisis de riesgos y evaluación de impacto**: estas obligaciones parten del principio de responsabilidad proactiva, presente en el RGPD, por el cual, el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con el RGPD y garantice la protección de los derechos de los usuarios. Para esto último, el análisis de riesgos se convierte en un elemento fundamental pues establece que medidas de protección son necesarias afrontar desde el diseño del tratamiento de datos hasta la continua evolución que pueda ir sufriendo a lo largo del tiempo (gestión continua de riesgos). El RGPD en su artículo 32 establece como medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, entre otras:

a) la seudonimización[15] y el cifrado de datos personales.
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

[15] Según el RGPD: "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*".

Así también, los controles de autenticación y política de protección de contraseñas tienen un papel relevante en las medidas de seguridad a implementar. Según recomendaciones emitidas por la Agencia Española de Protección de Datos (2018c):

> Por un lado, la aplicación debe implementar un mecanismo de autenticación que permita la identificación inequívoca y personalizada de los usuarios, recomendándose que este mecanismo consista en códigos de usuario y contraseñas, evitando la identificación de menores mediante datos biométricos (reconocimiento facial o huella dactilar).
>
> Si se utilizan contraseñas, el Centro debe incluir en su política el cambio periódico de las mismas, por lo que las aplicaciones que se vayan a utilizar deben incluir mecanismos para permitir dichos cambios. A los usuarios les corresponde la obligación de utilizar de contraseñas robustas y custodiarlas sin desvelarlas a terceros. (p.11)

Tanto *G Suite for Education* como *Microsoft Office 365* permite al responsable configurar a través de las respectivas consolas de administración una política de contraseñas propia estableciendo, entre otros parámetros, la longitud, el plazo de expiración, la necesidad de utilizar caracteres especiales, etc.

Debido a la complejidad de algunas de estas medidas no es necesario decir que el encargado del tratamiento asume un papel relevante en el análisis de riesgos y en la incorporación de medidas de control y seguridad. En nuestro caso, las dos plataformas examinadas cumplen con estándares de seguridad de la información (ISO/IEC 27001[16], ISO/IEC 27017[17], ISO/IEC 27018[18]) y auditorías externas (SOC[19]), además de declarar en sus respectivas Adendas de protección de datos la implementación de un amplio catálogo de medidas de seguridad, entre otras:

- Obligaciones de confidencialidad por parte del personal.
- Protección contra interrupciones.
- Procedimientos de recuperación de datos.

[16] https://www.iso.org/isoiec-27001-information-security.html

[17] https://www.iso.org/standard/43757.html

[18] https://www.iso.org/standard/76559.html

[19] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

- Control de software malicioso.
- Cifrado de datos.
- Notificaciones ante cualquier incidente.

Con respecto a las evaluaciones de impacto relativas a la protección de datos (en adelante, EIPD), definida por la Agencia Española de Protección de Datos (2018b) como:

> Una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable. (p.4)

La EIPD, no parece ser, a priori, una obligación prescriptiva en el uso de las plataformas educativas analizadas, al no caer dentro de los supuestos establecidos en el artículo 35.3 del RGPD que requieren de su aplicación.

- **Designación de un delegado de protección de datos**: obligación en consonancia con el principio de responsabilidad proactiva del RGPD. La LOPDGDD en su artículo 34.1 establece que los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

Entre las funciones más importantes que se le asignan al DPD se encuentran las de informar, asesorar y supervisar el cumplimiento de la normativa sobre protección de datos, así como la de resolver reclamaciones que se puedan plantear, además de ser el interlocutor con la AEPD y con los interesados. Para el cumplimiento de sus funciones y poder armonizar los tratamientos de datos personales en los centros educativos, las dudas que puedan surgir han de

trasladarse al delegado de protección de datos (Agencia Española de Protección de Datos, 2018, p.11).

7. Conclusiones

En este artículo, hemos analizado dos de las plataformas para el aprendizaje más utilizadas en nuestro país por los centros educativos: *G Suite For Education* y *Office 365 Education*. Y en ambos casos, ha quedado patente que las dos plataformas cumplen con las exigencias que hoy en día establecen tanto el Reglamento europeo como la legislación nacional en relación con la protección de datos personales. Por consiguiente, desde un punto de vista teórico, sería imposible afirmar que la información proporcionada por el alumnado y el profesorado pueda estar expuesta a filtraciones o mal uso, sin cuestionarnos la normativa actual que regula esa protección. Pero como hemos visto, desde un punto de vista práctico, la protección de los datos personales se sustenta en un conjunto más amplio de responsabilidades que no solo abarca al encargado del tratamiento. En tal sentido, el principio de responsabilidad proactiva del responsable de los datos, ya sea la Administración o los titulares del centro privado, analizando los posibles riesgos y cumpliendo con las distintas medidas técnicas y organizativas en su ámbito de actuación, se vuelven indispensables.

En base a lo anterior, es el responsable el primero que debe garantizar los principios de licitud, lealtad y transparencia, proporcionando toda la información de una manera entendible y sencilla, explicando a su vez cual es la finalidad de la recogida de los datos y vigilando que sean los adecuados, pertinentes y limitados a lo necesario.

Asimismo, se revela como fundamental el establecimiento de un límite temporal para la conservación de los datos personales y posterior eliminación, así como de las copias de datos generadas, y el permitir que los usuarios puedan ejercitar sus derechos.

De igual forma, es importante la selección de servicios y aplicaciones adicionales que puedan añadirse a las plataformas analizadas, realizando, previamente a su incorporación, un análisis de la política de privacidad que incorporan por si pudieran presentar riesgos con respecto a la protección de datos personales, y solicitando el

respectivo consentimiento si la legitimación de su uso cae fuera del estricto ejercicio de la función educativa.

Como vemos, un agregado de responsabilidades individuales y otras conjuntas que no pueden ser atribuidas exclusivamente al encargado del tratamiento, en nuestro caso *G Suite For Education* o *Office 365 Education*, y que bien aplicadas van a determinar seguridad para los usuarios en el uso de estas plataformas educativas, de conformidad con las políticas de privacidad aceptadas y dentro del marco general de protección que proporciona el Reglamento europeo y la legislación nacional. Posibilitando, además, que ante cualquier vulneración las autoridades de control de los respectivos países, en caso de España la Agencia Española de Protección de Datos, pueda abrir expedientes por infracción y en su caso imponer sanciones cuantiosas, como así ha sucedido a nivel internacional.

Financiación

Sin financiación expresa.

Conflicto de intereses

El autor pertenece al Consejo de Redacción de la revista Avances en Supervisión Educativa.

Referencias bibliográficas

Acuerdo de G Suite for Education (2020). *Condiciones de Servicio de G Suite*. https://gsuite.google.com/terms/education_terms.html

Adenda de Tratamiento de Datos (2020). *G Suite and Complementary Product Data Processing Amendment, Version 2.2*. https://gsuite.google.com/intl/es/terms/dpa_terms.html

Adenda de Protección de datos de servicios online de Microsoft (2020). *Online Services Data Protection Addendum (DPA)*. https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=16059

Agencia Española de Protección de Datos (2018). *Guías sectoriales AEPD. Guía para centros educativos*. https://www.aepd.es/sites/default/files/2019-10/GuiaCentrosEducativos.pdf

Agencia Española de Protección de Datos (2018b). *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Agencia Española de Protección de Datos (2018c). *Informe sobre la utilización por parte de profesores y alumnos de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas*. https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-apps-datos-alumnos.pdf

Autoridad Catalana de Protección de Datos (2018). *Pautas de protección de datos para los centros educativos*. https://apdcat.gencat.cat/web/.content/04-actualitat/menors-i-joves/documents/GUIA-PAUTAS-DE-PROTECCION-DE-DATOS-PARA-CENTROS-EDUCATIVOS.pdf

G Suite for Education (2020). *G Suite for Education*. https://edu.google.com/intl/es-419/products/gsuite-for-education/?modal_active=none

Office 365 Education (2020). *Microsoft Educación*. https://www.microsoft.com/es-es/education/products/office

Referencias normativas

Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (BOE núm. 274, de 15 de noviembre de 1985). https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 262, de 31 de octubre de 1992). https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario

Oficial n° L 281 de 23/11/1995). https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=ES

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14 de diciembre de 1999). https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Reglamento de la Unión Europea (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial de la Unión Europea L 119, de 4 de mayo de 2016).https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 6 de diciembre de 2018). https://www.boe.es/eli/es/lo/2018/12/05/3/con