

MENORES, PRIVACIDAD Y DERECHOS HUMANOS EN LA ESCUELA. EL CASO DE GOOGLE WORKPLACE FOR EDUCATION EN ESPAÑA

MINORS, PRIVACY AND HUMAN RIGHTS AT THE SCHOOL.
THE CASE OF GOOGLE WORKPLACE FOR EDUCATION IN SPAIN

RAFAEL RODRÍGUEZ PRIETO
Universidad Pablo de Olavide, Sevilla
<https://orcid.org/0000-0002-8056-1785>

Fecha de recepción: 1-12-22
Fecha de aceptación: 17-5-23

Resumen: *Este artículo analiza la aplicación en la escuela de plataformas privadas de enseñanza, cuyo uso ha tenido un impulso con la pandemia de la COVID19. Google workplace for education se ha considerado una vía eficaz tanto para adaptarse a los retos de la digitalización como para afrontar situaciones extraordinarias. El análisis realizado revela una amenaza ligada a la intimidad de los menores. Aplicando análisis heurístico, los resultados muestran la necesidad de efectivizar un principio de cautela tecnológica sobre el uso de estas plataformas en la educación. Se concluye con la necesidad de profundizar en el análisis de las implicaciones para los niños y adolescentes del uso de este software y la conveniencia de aplicar herramientas libres y abiertas.*

Abstract: *This paper analyzes the use in schools of private teaching platforms. They have had a boost with the COVID19 pandemic. The use of Google workplace for education has been considered an effective way both to adapt to the challenges of digitization and to face critical situations. The analysis carried out reveals a threat linked to the privacy of minors. Applying heuristic analysis, the results show the need to implement a principle of technological caution on the use of these platforms in education. It concludes with the need to deepen the analysis of the implications for kids and teenagers of the use of this software and the convenience of applying free and open tools.*

Palabras clave: internet, Google, plataformas educativas, intimidad, menores
Keywords: internet, Google, educative platforms, privacy, minors

1. INTRODUCCIÓN¹

Hace unos meses, un medio de comunicación se hacía eco de una curiosa respuesta de un asistente de voz. Una madre nerviosa preguntó: “Alexa, ¿cómo consigo que mis hijos dejen de reírse?” La respuesta fue: “Según un colaborador de *Alexa Answers*, si es conveniente, podrías darles un puñetazo en la garganta”. Y el asistente de voz de Amazon continuó: “Si se retuercen de dolor y no pueden respirar, será menos probable que se rían”. La conversación, según el periódico, se difundió mediante la red social china TikTok².

El medio apuntaba a la necesidad de mejora de ciertos protocolos vinculados a la moderación de contenidos. Pero más allá de cuestiones técnicas, existe una creciente preocupación por la influencia de internet en el desarrollo de la infancia y la adolescencia. Recientemente, se ha alertado del impacto del visionado de vídeos pornográficos en los menores³ o de los suicidios como consecuencia del acoso escolar. También ha de ser tenida en consideración el uso de internet para la comisión de delitos de diverso tipo. En este sentido, la Agencia Española de Protección de Datos (AEPD) publicó una serie de recomendaciones muy prácticas para evitar el acceso del menor a contenido inapropiado⁴. Estas se encuentran vinculadas con la protección de su privacidad que es un derecho recogido en el art. 4 de la Ley del Menor⁵.

¹ Este artículo ha sido financiado por el Fondo Europeo de Desarrollo Regional (FEDER) y por la Consejería de Economía, Conocimiento, Empresas y Universidad, de la Junta de Andalucía, en marco del programa operativo FEDER Andalucía 2014-2020. Objetivo específico 1.2.3. “Fomento y generación de conocimiento frontera y de conocimiento orientado a los retos de la sociedad, desarrollo de tecnologías emergentes”) en marco del proyecto de investigación de referencia UPO-1380664. Porcentaje de cofinanciación FEDER 80%.

² <https://elpais.com/tecnologia/2022-11-07/podrias-darles-un-punetazo-en-la-garganta-el-consejo-de-alexa-a-una-madre-para-calmar-a-sus-hijos.html>. Esta red social ha tenido un fuerte crecimiento en Europa y EE.UU., lo que ha generado cierta preocupación en relación a los datos que se envían a China, lugar de la sede de la empresa. No obstante, también debería llamar la atención el contraste entre los contenidos que ofrece esta red social en China –formativos, en general– y los que distribuye en el resto del mundo, banales y, en ocasiones, hasta peligrosos, por los retos absurdos que se convierten en virales y terminan dañando a los que los intentan.

³ L. BALLESTER BRAGE y C. ORTE SOCIAS, *Nueva pornografía y cambios en las relaciones interpersonales*, Octaedro, Barcelona, 2019.

⁴ AEPD, *Protección del menor en internet*, <https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf>

⁵ Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

Niños y adolescentes cuentan con una protección de su intimidad que se concreta en una serie de límites en el acceso a sus comunicaciones.

Otro aspecto que también debe ser tomado en cuenta es el de los problemas psicológicos derivados de un abuso de las pantallas. De hecho, ya existen estudios que los concretan en diversas psicopatías que afectan cada vez más a niños y niñas. La extensión del teléfono móvil provoca escenas tan comunes como la que muestra a una familia sentada a la mesa de un restaurante sin apenas hablarse, ya que todos están mirando la pantalla de su dispositivo electrónico. Y tampoco es suficiente con pedir a los niños que guarden sus teléfonos; se trataría de establecer una comunicación que englobe algo que es esencial entre generaciones: la transmisión de nuestras experiencias y propiciar una reflexión sobre el uso de la tecnología⁶.

De estos ejemplos se pueden extraer dos consecuencias fundamentales. La primera es la necesidad de proteger a este sector poblacional en internet. La segunda sería generar una conciencia social mayor sobre los riesgos de la Red. Esta investigación se ocupa de la primera, aunque la educación y la formación es tan necesaria como la garantía de bienes jurídicos, básicos para la preservación de una sociedad democrática. Este trabajo se propone analizar el uso en la escuela de la plataforma educativa *Google workplace for education*. La hipótesis de este artículo es que se debiera aplicar un principio de ‘cautela tecnológica’, ya que existen dudas razonables en cuanto a la garantía de protección derechos de menores en el ámbito escolar. Tampoco es baladí la cuestión de si es razonable que se les aculture en el uso de plataformas privadas y cerradas, en vez de software libre, que podría ser auditado tanto por profesores como por sus progenitores y otros miembros de la sociedad civil. Como ha señalado Asís Roig, igualdad y no discriminación cuentan con dos proyecciones diferentes y relacionadas. La primera se concreta en la igualdad de acceso a las nuevas tecnologías. La segunda, puede servir para “acrecentar las diferencias de poder, capacidad y bienestar de los seres humanos”⁷.

El art. 7 de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales prevé que el tratamiento de los datos personales de un menor solo se podrá fundar en su consentimiento cuando sea mayor de catorce años. Se exceptúan aquellos supuestos en que,

⁶ S. TURKLE, *Reclaiming Conversation: The Power of Talk in a Digital Age*, Penguin, New York, 2016, p. 14.

⁷ R. DE ASIS, *Derechos y tecnologías*, Dykinson, Madrid, 2022, p. 21.

con arreglo a la ley, se establezca la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico debido a que se precisa el consentimiento para el tratamiento de los datos. En el caso de los que cuentan con menos de catorce años, solo será lícito recabar fundados en el consentimiento, si consta el del titular de la patria potestad o de la tutela. De acuerdo con esta legislación, los centros educativos y otros que cuenten con actividades donde participen menores de edad han de garantizar la protección de su interés y de sus derechos fundamentales (art. 92). El considerando 38 del Reglamento de Protección de Datos de la UE establece que los menores merecen una protección específica⁸. Los propios titulares de la patria potestad no son excluidos de esta garantía. Por ejemplo, a partir de los 14 años⁹, los padres deben contar con el consentimiento de hijos e hijas para acceder a sus redes sociales. Solo se permitiría obviar esta obligación en caso de un riesgo evidente que hiciera necesaria su intervención con el fin de protegerlos. Existe una interesante jurisprudencia que justificaría este tipo de intromisión (acceso a cuentas en redes sociales), que detalla Toral Lara¹⁰.

En este trabajo se utiliza el método sociológico jurídico. Su uso se justifica por la necesidad de identificar las obligaciones jurídicas. Así, se trata no solo de profundizar en la cuestión de los derechos fundamentales y, más concretamente, en la protección de datos, sino que también se recurrirá a otras ciencias conexas como, la ciencia de la educación, la sociología o la económica, con el fin de desarrollar una explicación que englobe tanto al hecho jurídico como su eficacia.

⁸ Reglamento de Protección de Datos por la UE 2016/679 de 27 de abril de 2016. Otra legislación aplicable sería la Ley 34/2002 de 11 de julio sobre Servicios de la Sociedad de la Información y Comercio Electrónico, en la que se establece que se deben adoptar todas las medidas necesarias para proteger a la infancia y a la juventud en internet.

⁹ De acuerdo a la doctrina, a partir de los 12 años el menor puede contar con la madurez suficiente para ser consciente de su dignidad, lo que implica valorar su privacidad, condicionando por ello la capacidad de los progenitores de control sobre sus comunicaciones (L. A. GODOY DOMÍNGUEZ, “El conflicto entre el derecho a la intimidad de los menores en el uso de las TICs y el cumplimiento de los deberes de la patria potestad”, *Actualidad civil*, vol. 12, 2018, pp. 1-22).

¹⁰ E. TORAL LARA, “Menores y redes sociales: consentimiento, protección y autonomía”, *Derecho Privado y Constitución*, núm. 36, 2020, pp. 179-218. En especial 209-211. Como señala Toral Lara, “excepcionalmente, las intromisiones se considerarán legítimas si buscan proteger el interés superior del menor o bienes o derechos de terceros. Estas intromisiones deben ser proporcionadas a los males que se pretenden evitar, y en todo caso debe tratar de obtenerse el consentimiento del menor”.

Tal como se ha afirmado en relación a la economía, el derecho no puede estudiarse como un dominio aislado, sino que debe analizarse en relación con la realidad social, no como una mera parte de ésta¹¹. En este sentido, cualquier conocimiento racional de lo humano implica el reconocimiento de lo que en él excede¹². Como consecuencia de esta perspectiva metodológica se acudirá al método valorativo, con el fin de interpretar el derecho vinculando elementos relacionados con sus principios básicos y axiología. Estos parámetros nos permiten identificar, de una forma más exacta, obligaciones jurídico-democráticas.

Asistentes de voz como el protagonista de la noticia anterior son una mina de captación de datos para las empresas que los fabrican. Recientemente, la inteligencia artificial dialógica ChatGPT fue prohibida en Italia por contravenir la legislación de protección de datos y detectar una pérdida de datos tanto de usuarios ocasionales como de sus abonados en día 20 de marzo. No es extraño que algo así suceda, cuando se pone en circulación un software como este, para que la legislación actual no parece preparada¹³.

Los usuarios deberían conocer las condiciones en las que los tienen en casa y la influencia que pueden tener. Más allá de consejos inhumanos, como el descrito al inicio de este artículo, debería cuestionarse la oportunidad de que una máquina capte y transmita diariamente la actividad de un hogar donde, a veces, viven menores. En el caso del entorno escolar, se debieran extremar las cautelas. Si los propios titulares de la patria potestad están condicionados por nociones como la edad o madurez de sus hijos e hijas para invadir su privacidad, se debería ser igualmente exigente con los centros educativos públicos y su obligación de guardia y custodia. Sería paradójico castigar a unos progenitores que acceden a datos personales de sus hijos, excediéndose en su celo, y permitir, al mismo tiempo, que una empresa pri-

¹¹ G. CABIESES CROVETTO, "El carácter interdisciplinario del derecho y la utilidad de la economía en su estudio". *Themis*, núm. 62, 2012, pp. 11-25, <https://n9.cl/q7bn6>

¹² E. MORIN, *El método 5. La humanidad de la humanidad. La identidad humana*, Cátedra, Madrid, 2008, p. 321.

¹³ <https://www.xataka.com/legislacion-y-derechos/italia-ha-abierto-camino-ahora-gobiernos-europeos-se-plantean-prohibir-chatgpt> Un mes después de su bloqueo, Italia permitió su reactivación de acuerdo a una serie de condiciones. La autoridad italiana de protección de datos lamentó la falta de verificación de la edad de acceso a la herramienta –algo que se ha convertido en un mal endémico de internet–, junto con la falta de una base jurídica que justifique la recogida y conservación de los datos de sus usuarios.

vada pueda acumularlos y procesarlos sin que tengamos plenas garantías de que no afecta a sus derechos fundamentales.

2. MENORES E INTERNET. ¿RIESGOS PARA LOS DERECHOS HUMANOS?

La pandemia de la COVID19 ha incrementado el interés de los centros educativos por la utilización de plataformas de enseñanza online. La posibilidad de obtener un paquete cerrado que permitiera atender necesidades de enseñantes y alumnado durante el periodo de confinamiento generó una fuerte demanda. La idea de que la digitalización permanecerá más allá de este tiempo parece también haberse fortalecido, junto con la necesidad de que se afronte una necesaria, y cada vez más urgente, alfabetización digital que minimice los efectos indeseados del uso de estas tecnologías en el rendimiento escolar¹⁴.

En este contexto, Google, que domina la industria del conocimiento de forma similar a Amazon en el caso de la venta online¹⁵, ofreció un paquete para resolver los problemas derivados de la digitalización en la escuela y generar una enseñanza semipresencial o a distancia. Noticias como el abandono de la plataforma Educa Madrid por parte de los docentes, a causa de sus deficiencias, y el paso a plataformas de Microsoft y Google o el uso en Cataluña de estas plataformas antes de la pandemia, generó la intervención de la Administración pública, en el primer caso, o de organizaciones de la sociedad civil, en el segundo. Así, en el inicio del curso académico 2020/21, la Consejería de Educación de la Comunidad de Madrid prohibió el uso de las, denominadas en prensa como plataformas “gratuitas”, aunque su calificación más exacta sea privativas¹⁶.

Las razones que se esgrimieron fueron que existiría un incumplimiento de la normativa de protección de datos, junto con un desafío de la jurisprudencia del Tribunal de Justicia de la UE (TJUE) –cabe citar el Asunto C-311/18 - *Data*

¹⁴ D. HALPERN, et al., “El rendimiento escolar: Nuevos recursos multimedia frente a los apuntes tradicionales.” *Comunicar*, núm. 64, 2020, pp. 39-48. 64, <https://doi.org/10.3916/C64-2020-04>

¹⁵ S. GALLOWAY, *The Four. The Hidden DNA of Amazon, Apple, Facebook and Google*, Bantam Press, London, 2017, p. 176.

¹⁶ Lo gratuito en internet no existe o es muy minoritario. Se paga con los datos. Desgraciadamente, la falsa idea de la gratuidad de internet ha calado fuertemente en la juventud y también en los adultos. Sería imprescindible una educación sobre internet que destierre estos errores.

Protection Commissioner contra Facebook Ireland y Maximillian Schrems, que anula la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. Los docentes respondieron que sin esas plataformas no podían realizar su trabajo. En junio de 2019, organizaciones como Xnet solicitaron a los progenitores de Cataluña que no firmaran la autorización para el uso de la plataforma educativa de Google (en aquel momento se denominaba *Google Suite*). Además, requirió una alternativa a la consejería del ramo un año más tarde. Google respondió que los datos no se utilizarían para orientar la publicidad ni se divulgarían sin el consentimiento de los progenitores o tutores. Además, subrayó que la jurisprudencia del TJUE, avalaría la validez de las cláusulas contractuales estándar adoptadas por la Comisión Europea para realizar transferencias internacionales de datos entre un responsable establecido en la UE y un encargado del tratamiento fuera de ella¹⁷. Sin embargo, el TJUE invalidó el escudo de protección en julio de 2020¹⁸, lo que complicó la situación¹⁹.

En octubre de 2020, Google cambió el nombre de su plataforma para empresas: de *Google Suite* pasó a denominarse *Google Workplace* y en febrero de 2021 renombró la plataforma educativa como *Google Workplace for Education*. El cambio se justificó por una serie de mejoras técnicas que ampliarían las posibilidades de la enseñanza a través de internet. Por ejemplo, en el rediseño del servicio de videoconferencia o de *Google Classroom*, junto con el establecimiento de límites que afectaban a la política de almacenamiento de datos. A finales de 2020, la Consejería de Educación de la Junta de Andalucía firmó un acuerdo con Google y Microsoft para que durante dos años prorrogables los centros docentes públicos andaluces puedan acceder a sus plataformas educativas. Dicho acuerdo se encuentra vigente en la actualidad²⁰.

¹⁷ No está tan claro que estas cláusulas estén avaladas. De hecho, en febrero de 2022, Meta amenazó a la UE con la posibilidad de que Facebook o Instagram dejaran de prestar servicio en territorio de la UE. La razón es la personalización de los anuncios que constituye una de las principales fuentes de ingreso de sus redes sociales.

¹⁸ El 16 de julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) anuló la Decisión 2016/1250 de la Comisión que consideró adecuado el nivel de protección del Escudo de Privacidad (*Privacy Shield*) para las transferencias internacionales de datos a EEUU (<https://curia.europa.eu/juris/documents.jsf?num=C-311/18>).

¹⁹ El 7 de octubre de 2022, el Presidente de EE.UU. firmó una orden ejecutiva cuyo fin era resolver los problemas de los datos transferidos desde la UE a EE.UU. El objetivo es garantizar que los datos transferidos a EE.UU gozarán de un estándar alto de protección.

²⁰ https://www.juntadeandalucia.es/sites/default/files/2021-01/Convenio_30.pdf El punto d establece que "Google podrá almacenar y tratar los datos en cualquier lugar en el que Google

Se trata de una situación que genera tanto expectativas como preocupación, junto con unas fuertes dosis de incertidumbre por los riesgos que pudiera entrañar. Por un lado, tenemos buena parte de la comunidad educativa que entiende que, a falta de unas herramientas públicas adecuadas para garantizar el derecho constitucional a la educación, se deben usar este tipo de plataformas, ya que son eficientes y sirven para el cumplimiento de este derecho. No obstante, al contrario que en la práctica habitual en internet donde decidimos firmar o no un contrato de adhesión con una plataforma, en la enseñanza obligatoria, los progenitores o tutores, se pueden ver, en cierta forma, compelidos a la aceptación de los términos y condiciones de uso de plataformas como la que nos ocupa (exceptuados “los comprendidos entre aquellos que los centros docentes pueden recabar del alumnado de conformidad con la disposición adicional 23ª de la Ley Orgánica 2/2006, de 3 de mayo, de Educación” -7.6 del Acuerdo Junta-Google) si no quieren perjudicar la educación de sus hijos. Así, surge la preocupación por los bienes jurídicos en juego. Por un lado, se ha de analizar la protección de los datos de los menores y la introducción de un tercero en la educación, ajeno a la comunidad educativa y a la Administración; por otro, la garantía del derecho a la educación, evitando cualquier tipo de discriminación o de quiebra del mismo, por razones de clase o tecnológicas.

Toda esta polémica coincide además con una notable inquietud por la gestión del uso de las pantallas en niños y adolescentes o los daños que pueden generar en su desarrollo²¹. La promoción, por parte de los dirigentes políticos, de la inserción de tecnología de este tipo en el aula debería someterse a escrutinio y análisis. No es que se trate de una mala idea; más bien la razón estriba en someter a deliberación pública y a argumentos científicos y garantistas cualquier política pública y, en especial, aquella que afecta a derechos fundamentales. Como señala Mosco en su análisis del mito de la digitalización, no se trata meramente de un término antropológico, sino político, que transmite ideología a los valores humanos. Es importante analizar lo que un mito revela de una sociedad²².

o sus subencargados tengan instalaciones, con sujeción a las obligaciones sobre transferencias de datos establecidas en el artículo 10 de la Adenda del Tratamiento de Datos”, lo que no garantiza que los datos de los menores permanezcan en espacio de la UE. Para el curso 2022/23 se han ofertado nuevas opciones. Por ejemplo, los docentes pueden añadir una foto o un apodo a su perfil. <https://www.juntadeandalucia.es/educacion/eaprendizaje/gsuite/>

²¹ M. DESMURGET, *La fábrica de cretinos digitales*, Barcelona, Península, 2022, pp. 344-350.

²² V. MOSCO, *The Digital Sublime. Myth, Power, and Cyberspace*, Cambridge, The MIT Press, 2004, pp. 30-31.

La UE, en su reciente reglamento sobre servicios digitales, afirma en el considerando (35) que,

“el presente Reglamento establece obligaciones básicas aplicables a todos los prestadores de servicios intermediarios, así como obligaciones adicionales para los prestadores de servicios de alojamiento de datos y, más concretamente, los prestadores de plataformas en línea y de motores de búsqueda en línea de muy gran tamaño. (...) Esas obligaciones armonizadas de diligencia debida, que deben ser razonables y no arbitrarias, son necesarias para cumplir los objetivos de interés público que se hayan determinado, como la salvaguardia de los intereses legítimos de los destinatarios del servicio, la lucha contra las prácticas ilícitas y la protección de los derechos fundamentales consagrados en la Carta. Las obligaciones de diligencia debida son independientes de la cuestión de la responsabilidad de los intermediarios y, por tanto, deben apreciarse por separado”²³.

Es importante tener en cuenta que la intimidad de niños y adolescentes es un elemento esencial de sus derechos como tales y deben ser susceptibles de una atención muy especial por el legislador y las administraciones públicas. Resulta de singular importancia, la protección de aquellos que padecen algún tipo de discapacidad, lo que los haría aún más vulnerables. En este sentido, un estudio de la Universidad de Alicante muestra que las personas discapacitadas, por su ingenuidad y credulidad social pueden tener un grado mayor de vulnerabilidad en el uso de internet²⁴.

Conviene aclarar que este concepto -intimidad- es el más utilizado en derecho español, aunque en los últimos años, por influencia de *EE.UU.*, se tiende a la utilización del concepto privacidad. Polo Roca, señala que “el concepto estadounidense de derecho a la privacidad o intimidad (*right to privacy*) es lo mismo que el español derecho a la intimidad (en sentido amplio)” y el término de privacidad de los datos (*data privacy*) equivaldría, “mutatis mutandis, al término protección de datos (*data protection*)”²⁵.

²³ https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_ES.html#title2

²⁴ VV.AA., *Internet y discapacidad intelectual: riesgos y preocupaciones desde la perspectiva de las familias y de los profesionales*, ACIPE, 2016, <https://rua.ua.es/dspace/handle/10045/64550>

²⁵ A. POLO ROCA, “Privacidad, intimidad y protección de datos: una mirada estadounidense y europea”, *Derechos y Libertades*, núm. 47, 2022, pp. 307-338. En este trabajo se usará el concepto de privacidad en razón del objeto de estudio ligado al análisis de un acuerdo para que una compañía estadounidense se encargue de datos de menores españoles al facilitar un servicio educativo.

Más allá de precisiones terminológicas, se ha de insistir en la relevancia que una adecuada protección de la intimidad o privacidad tiene en el desarrollo de la persona y en su dignidad. Según Blázquez, uno de los mayores retos de la sociedad digital es examinar el uso secundario que pudiera hacerse de la información proveniente de los datos personales²⁶, aunque, como afirma Gil Antón, “la privacidad está cada vez más expuesta y, en ocasiones, ni siquiera se exige un comportamiento intencionado por parte del usuario”²⁷. Así, Moreno Bobadilla señala que el caso de niños y niñas se requeriría de una especial protección, ya que pueden no calibrar de forma adecuada las consecuencias de sus publicaciones en la Red²⁸.

La brecha digital o la falta de igualdad de oportunidades en el acceso, es decir en la calidad de la conexión y la adquisición del material necesario para la misma, son también relevantes y han recibido la atención del legislador en programas específicos. Sin embargo, faltan análisis que se centren en la protección de los datos de los estudiantes en el ecosistema educativo y los bienes jurídicos en juego. La inserción de empresas privadas con ánimo de lucro lo aconsejaría. Este trabajo se ocupa de esta última línea de investigación y ofrece vías para la protección de nuestros menores, mediante la aplicación de un principio de precaución de índole tecnológico. El uso de plataformas educativas diseñadas por entidades privadas con ánimo de lucro, debe observar un principio de precaución en analogía con otras áreas del derecho como el medioambiental. El derecho que se deriva de los poderes legislativos de los Estados nación democráticos tiene en internet y sus procesos un desafío que le afecta de forma directa en cuestiones tan básicas como la tutela judicial efectiva, el estatuto jurídico de servidores y centros de procesamiento de datos o las transformaciones en la privacidad y la globalidad del cableado de la Red. Hay en juego derechos personalísimos que, en el caso de niños y

²⁶ F. J. BLÁZQUEZ RUIZ, “Riesgos para la privacidad en la aplicación de la inteligencia artificial al ámbito biosanitario. Implicaciones éticas y legales”, *Anales de la Cátedra Francisco Suárez*, núm. 56, 2022, pp. 245-268.

²⁷ A. M. GIL ANTÓN, “La privacidad del menor en internet”, *Revista de Derecho, Empresa y Sociedad (REDS)*, núm. 3, 2013, pp. 60-96.

²⁸ A. MORENO BOBADILLA, *Intimidad y menores*, Centro de estudios Políticos y Constitucionales, Madrid, 2017, p. 164. En el último capítulo, la autora reflexiona sobre las debilidades de la legislación y la jurisprudencia para proteger a los menores en su vida online. Es extremadamente desconcertante que el legislador haya establecido tantos obstáculos para que los padres intervengan en la vida online de sus hijos y se haya preocupado tan escasamente de su protección en el ámbito de internet. No es extraño que las consecuencias tengan forma de suicidios o abusos de todo tipo.

adolescentes, exigen además una especial cautela, lo que debería reforzar la regulación en este ámbito.

3. DE LA DIGITALIZACIÓN ACRÍTICA A LA EXIGENCIA DE DERECHOS FUNDAMENTALES EN LA RED: MENORES Y PLATAFORMAS DE ENSEÑANZA PRIVATIVA

La Constitución española en su artículo 27.2 afirma que: “La educación tendrá por objeto el pleno desarrollo de la personalidad humana en el respeto a los principios democráticos de convivencia y a los derechos y libertades fundamentales”. Junto con este punto cabe resaltar, en relación al objeto de nuestra investigación, tanto el punto 4 como el 9. El primero declara la obligatoriedad y gratuidad de la enseñanza básica. En 9 establece que los poderes públicos tienen la obligación de ayudar a los centros docentes para que reúnan los requisitos que la ley establezca. Una de las primeras cuestiones que se extraen del articulado es la necesaria intervención pública en la garantía de una infraestructura mínima para el cumplimiento de los preceptos constitucionales²⁹ que con el uso de la educación online se amplía por la necesidad de que la infraestructura de comunicación sea estable y garantice la recepción y emisión en igualdad de circunstancias.

La Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOMLOE) toma la competencia digital como principio pedagógico transversal en la educación básica (artículo 19.2 y 24.5, de la LOE modificado por la LOMLOE). También se garantiza el derecho a la educación digital en el artículo 83 de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales. En el preámbulo de la primera se establece que la Ley tendrá en cuenta el cambio digital. Se establece que la competencia digital incluye tanto “el dominio de los diferentes dispositivos y aplicaciones” como “la atención al desarrollo de la competencia digital de los y las estudiantes de todas las etapas educativas, tanto a través de contenidos específicos como en una perspectiva transversal, y haciendo hincapié en la brecha digital de género” (LOMLOE, Preámbulo).

El desarrollo de esta competencia se incluye como un principio pedagógico (artículo 19), junto a la preparación del “alumnado en materia de digitaliza-

²⁹ G. GÓMEZ ORFANEL, “Derecho a la educación y libertad de enseñanza. Naturaleza y contenido”, *Revista Española de Derecho Constitucional*, núm. 7, 1983, pp. 411-435, <https://n9.cl/q4kj>

ción en su sector productivo” (artículo 34). En el artículo 57 se prevé la adquisición de competencias digitales que faciliten una cultura digital en las aulas y evitando estereotipos de género. Es en este mismo artículo en su punto 7, en el que se establece que “las Administraciones públicas velarán por el acceso de todos los estudiantes a los recursos digitales necesarios, para garantizar el ejercicio del derecho a la educación de todos los niños y niñas en igualdad de condiciones”, estableciéndose una cláusula en la que se señala que “las tecnologías de la información y la comunicación (TIC) y los recursos didácticos que se empleen, se ajustarán a la normativa reguladora de los servicios y sociedad de la información y de los derechos de propiedad intelectual, concienciando en el respeto de los derechos de terceros”. Estas dos últimas previsiones configuran el sentido de la legislación educativa en materia digital. Por un lado, se establece que las Administraciones públicas deberán garantizar que el alumnado acceda a los recursos digitales en igualdad de condiciones. Por otro, que estos recursos podrán ser suministrados por terceros, por entes privados como la plataforma de la compañía que nos ocupa. Este tipo de recurso educativo consiste en un sistema tecnológico de comunicación multidireccional, que implica la integración de varios medios en uno (plataformas digitales y tecnológicas) y cuenta con espacios como el aula virtual³⁰.

Resulta de aplicación el Reglamento de Protección de Datos por la UE 2016/679 de 27 de abril de 2016, donde se establecen principios como el de minimización de datos, finalidad y responsabilidad proactiva. Estos principios responden a la necesidad de que los datos de carácter personal que se colecten han de ser los adecuados, pertinentes y deben limitarse al propósito para los que son tratados. Serán de aplicación medidas técnicas y organizativas apropiadas para que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento (artículo 25.2). El responsable de su tratamiento ha de ser diligente y llevar a cabo medidas técnicas y organizativas que lo garanticen, conforme con la legislación vigente (artículo 5.2). Así, la Administración educativa sería la responsable de este tratamiento de datos y el encargado, aquel con el que contrata el servicio. De acuerdo a Rubí, “las relaciones entre encargados y responsables del tratamiento se establecerán por medio de contratos de adhesión predispuestos por los primeros” y “frente a un particular afectado, el responsable primero no podrá oponer un tratamiento ajeno

³⁰ C. H. MARTÍNEZ URIBE, “La educación a distancia: sus características y necesidad en la educación actual”. *Educación* 33, vol. XVII, 2008, p. 24, <https://n9.cl/niupj>

a las instrucciones por parte de un contratista independiente”³¹. Todo ello, implica una responsabilidad de la Administración educativa y, por consiguiente, una necesidad de ser especialmente diligente tanto por tratarse de datos personales y de menores, como de encargar el servicio a una entidad externa, de acuerdo a un contrato de adhesión, denominado como ‘términos y condiciones de uso’.

En lo referido a la repercusión del consentimiento según la edad, se ha de señalar la diferencia entre los mayores de catorce años y el resto de los afectados. En el caso de los segundos, es necesaria la autorización del titular de la patria potestad o de la tutela. Junto a la edad, existe otra base que justifica el tratamiento de los datos al haber una relación contractual entre la Junta de Andalucía y Google. El problema reside en si los titulares de la patria potestad de los menores de 14 años cuentan con toda la información para prestar su consentimiento. Los términos y condiciones de uso son complejos y, a menudo, difícilmente comprensibles para personas que carecen de formación jurídica. Además, cabe señalar que es un consentimiento que no se ejerce en condiciones adecuadas ya que, en caso de que los progenitores o tutores no acepten, sus hijos no podrán seguir las clases como el resto del alumnado. La Administración educativa mantiene la responsabilidad de los datos de los menores y Google es la encargada de su tratamiento. Se requiere el consentimiento expreso de interesados o representantes cuando se trate de datos no comprendidos entre los que legalmente se pueden recabar del alumnado para prestar su función educativa³².

Google lleva años recolectando diferentes categorías de información de forma masiva y, en ocasiones, sin relación directa con su negocio³³. El

³¹ A. RUBÍ PUIG, “Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82”, *Revista de Derecho Civil*, núm. 4 vol. V, 2018, p. 67, <https://n9.cl/d186a>

³² Entre los datos que pueden recabar sin necesidad de un consentimiento expreso se encontrarían aquellos que hagan “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” (Disposición adicional 23, de la Ley Orgánica 2/2006, de 3 de mayo, de Educación). Esta disposición posibilita que prácticamente no sea necesario el consentimiento al ser muy amplio el abanico de datos que se pueden recabar de los estudiantes. Solo en el caso de contenido audiovisual, que parecería el único exceptuado de esta previsión legislativa, quedaría a valoración del responsable la petición del consentimiento.

³³ R. STROSS, *Planet Google. One Company's Audacious Plan to Organize Everything We Know*, Simon & Schuster, New York, 2008, p. 88.

control de la información es una cuestión sensible porque implica a derechos de carácter personalísimo. Su relevancia radica en su singular protección y en que no son renunciables. Las plataformas de agregaciones de herramientas como la que nos ocupa, suponen un paquete cerrado cuyo fin es cubrir las necesidades de la enseñanza. Su eficiencia a corto plazo es una de las razones de su uso. No obstante, se trata de una solución de carácter privativo, lo que significa que el programa no puede utilizarse con cualquier propósito, ni estudiarlo o modificarlo, con el fin de mejorarlo y, en definitiva, se limita la soberanía tecnológica de los ciudadanos³⁴. Estas opciones, que ofrece el software libre, no son posibles en este tipo de plataformas.

Las plataformas privativas, aprovechan el conocimiento que la mayoría de los usuarios tienen de las mismas, gracias a la omnipresencia de su software. Los Gobiernos autonómicos se han decidido por contratar este tipo de soluciones. La asociación Xnet, denunció la opacidad del uso de los datos por parte de Google en Cataluña. La alarma saltó cuando los titulares de la patria potestad recibieron un documento para que prestaran su consentimiento al uso del paquete de Google que incluye el procesador de texto para trabajos en equipo o un chat. El contrato de la empresa de San Francisco especifica que es necesario el consentimiento de los titulares de la patria potestad para el uso de servicios adicionales de *Workplace*. Para los principales, se deja al centro esa responsabilidad, ya que Google considera en su página de resolución de dudas que “cuando el centro educativo se registra en los servicios *de Google Workspace for Education* y los utiliza, se entiende que proporciona el consentimiento para usar los servicios principales en nombre de los padres”. La consecuencia es que los Gobiernos autonómicos permiten que los datos de los escolares terminen en servidores externos sobre los que no tienen ningún tipo de control. En realidad, solo cuentan con la promesa de la empresa de que actuará según el acuerdo firmado. La confianza que los progenitores o tutores depositan en la Administración educativa se “desplaza” de forma implícita a una empresa transnacional extranjera que va a tener una información muy relevante de sus hijos y que va procesar y tratar esos datos. Esta actividad les genera una relevante ventaja competitiva, además de aculturar a las nuevas gene-

³⁴ F. MARTÍNEZ CABEZUDO, “La educación virtual y la protección de los derechos fundamentales”, en R. SORIANO, R. y S. MARÍN CONEJO, S. (coord.), *El reto de los derechos humanos: Cuestiones actuales controvertidas*, Dykinson, Madrid, 2021, p. 89.

raciones su ecosistema, en vez de en la gestión colectiva de un procomún centrado en un conocimiento compartido³⁵.

En el Decálogo de UNICEF “Los e-derechos de los niños y las niñas”³⁶, se especifica en su punto 6 el derecho a la intimidad de las comunicaciones por medios electrónicos. El derecho a la imagen de los niños y adolescentes en internet es un elemento crucial que se vincula con la protección de sus datos personales. Los menores de 14 años precisan de una previa autorización paterna para registrarse cualquiera de los servicios que se ofrecen. Incluso se plantea la necesidad de establecer mecanismos de verificación de la edad del menor que accede a internet³⁷. Entendemos que existe una preocupación social que se ha reflejado en la Carta de Derechos Digitales de 2020. Se considera que hay una serie de riesgos y amenazas para los niños y adolescentes en el uso de la Red que implican actividades bien conocidas como el *bullying*, el uso de su imagen o el acceso a páginas de contenido violento o pornográfico. Hace unos meses, la Agencia Española de Protección de Datos actuó de oficio para multar con 525.000 euros a varias webs de contenido pornográfico por no disponer de mecanismo alguno que permita verificar el registro de un usuario de más de 14 años pero de menos de 18³⁸.

Es más difícil encontrar una reflexión sobre las indefiniciones y vaguedades que se derivan del uso de plataformas educativas. De hecho, existen estudios que afirman que los alumnos de entornos educativos más favorables hacen un uso más moderado de las nuevas tecnologías, lo que se traduce en un menor uso de las TIC para entretenimiento y una mayor propensión a su uso educativo³⁹, lo que supone reforzar la idea de la importancia del núcleo familiar en el éxito escolar.

³⁵ F. ORTEGA Y J. RODRÍGUEZ, *El potlatch digital. Wikipedia y el triunfo del procomún y el conocimiento compartido*, Cátedra, Madrid, 2011, p. 189.

³⁶ UNICEF, “Los e-derechos de los niños y las niñas”, <https://www.agamfec.com/decalogo-de-los-e-derechos-de-los-ninos-y-ninas/>

³⁷ M. M. HERAS HERNÁNDEZ, “Internet y el derecho al honor de los menores”. *Rev. IUS*, núm. 29 vol. 6, 2012, pp. 93-107. <https://n9.cl/fi3bq> En el caso de dictaduras como China, se han establecido controles en el acceso a internet de menores. Los juegos en línea solo son permitidos durante una hora, V. <https://www.latimes.com/espanol/internacional/articulo/2023-01-20/ninos-en-china-seguiran-solo-con-1-hora-de-juegos-en-linea>

³⁸ También fue multada por un uso de los datos personales que contravenía la legislación vigente. <https://www.aepd.es/es/documento/ps-00555-2021.pdf>

³⁹ D. MANZANO, D. Y M. FERNÁNDEZ-MELLIZO, “Origen familiar, uso del tiempo y de las tecnologías de la información”, *Revista Internacional de Sociología*, núm. 77, vol. 3, 2019, pp. 371-392.

Llama la atención que, por ejemplo, en la propuesta de UNICEF a la Carta de Derechos Digitales durante su consulta pública no se entrara en el uso de plataformas, cuando existen razones para ser cautelosos, si en caso de introducir a un tercero con ánimo de lucro en la educación de niños y niñas en tiempos en que un uso abusivo de las pantallas se ha revelado como un verdadero problema social. Nos situamos ante un escenario diferente y diverso. Lo primero en razón de que la influencia de las grandes corporaciones transnacionales privadas ha crecido de forma exponencial porque hoy tienen acceso a la vida íntima de cada ciudadano. Lo segundo porque las amenazas a su intimidad o privacidad no son meramente estatales. La capacidad de intromisión de estas empresas es hasta superior a los Estados y debiera contemplarse la posibilidad de que puedan llegar a acuerdos con ellos en beneficio de ambos y en perjuicio de los usuarios, sin descartar a otros actores como hackers o grupos criminales.

A veces se piensa que no existen alternativas solventes a estas empresas. Sin embargo, como señala Alex Hache, el uso de software libre genera curiosidad –modificar el software– y acultura en los estudiantes en la noción de cooperar y compartir el conocimiento⁴⁰. La escuela como centro para el desarrollo de un procomún tecnológico y cooperativo podría ser una alternativa que debiera, al menos, ser discutida y debatida racionalmente en la comunidad educativa. Una de las primeras ideas que se pueden extraer de esta cuestión es que, como en otros retos que afectan al desarrollo de esta tecnología, falta una deliberación pública sobre el impacto de internet en la sociedad y el papel regulador del derecho.

La necesidad de plantear un debate serio que incluya a la comunidad educativa en su conjunto ayudaría a que la Administración pública fuera especialmente cuidadosa y precavida cuando se trata de los derechos y el bienestar de menores de edad. Se podría establecer un paralelismo entre este tipo de cautela tecnológica y el principio de precaución en el ámbito del derecho ambiental. Ha sido la propia Comisión Europea la que lo ha adoptado en febrero de 2000, de acuerdo al art. 191 del Tratado de Funcionamiento de la UE. Este tipo de gestión del riesgo se establece en caso de una amenaza potencial y, en ningún caso, puede servir para justificar la toma arbitraria de decisiones. Así, la propia UE lo ha aplicado en cuestiones como el marco reglamentario de las sustancias químicas [Reglamento (CE) n.o 1907/2006;

⁴⁰ A. HACHE (ed.), *Soberanía tecnológica*, AH, Barcelona, 2014, pp. 39-40.

denominado REACH] y la legislación alimentaria general [Reglamento (CE) n.º 178/2002]⁴¹.

Corti Varela realizó un análisis de la jurisprudencia de la Corte Internacional de Justicia, Organización Mundial del Comercio y el Tribunal Internacional del Derecho del Mar, para examinar el impacto del principio de precaución sobre la carga de la prueba y su influencia en el estándar de revisión. La conclusión de su estudio fue que la jurisprudencia internacional entiende que su aplicación exige previamente la constatación tanto de la incertidumbre científica como de la gravedad del riesgo, cuya comprobación precisa de una correcta incorporación de la prueba científica⁴². Así, el principio de precaución ha adquirido un amplio respaldo en la práctica internacional lo que, para buena parte de la doctrina internacionalista, se traduce en un principio de derecho consuetudinario⁴³. Recientemente, López Pérez incidía en la necesidad de observar ciertas cautelas en el uso de drones en los espacios naturales por las consecuencias que pudiera tener para el medio ambiente de la zona afectada y las especies naturales⁴⁴. Como señala Salazar, “los efectos casi nunca son inmediatos, es necesario que transcurra un determinado tiempo para saber cuál fue la afectación real y cierta que se ocasionó”⁴⁵. En este sentido, Soro Mateo, invocando jurisprudencia comunitaria (STJUE *Pficer-Conseil*, de 11 de septiembre de 2002 –C-13/1999–), señala que la decisión pública sobre el riesgo permitido no debiera sustentarse únicamente el conocimiento científico existente, sino que debe acompañarse “de una reflexión ética, en la medida en que el principio de precaución tiene la virtualidad de transformar el contenido de la responsabilidad jurídica, que exige actuación y respuesta en casos de incertidumbre tan pronto como sea posible”⁴⁶.

⁴¹ V. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:precautionary_principle

⁴² J. CORTY VARELA, “Principio de precaución en la jurisprudencia internacional”, *Revista Española de Derecho Internacional*, núm. 69, 2017, p. 242, <http://dx.doi.org/10.17103/redi.69.1.2017.1.08>

⁴³ P. SANDS, *Principles of International Environmental Law. Vol.1*, Manchester, Manchester University Press, 1995, p. 212.

⁴⁴ F. LÓPEZ PÉREZ, “Restricciones aéreas en espacios naturales. Especial consideración a los drones”, *Revista Aranzadi de derecho ambiental*, núm. 51, 2022, pp. 145-182.

⁴⁵ B. ARCILA SALAZAR, “El principio de precaución y su aplicación judicial”, *Revista Facultad de Derecho y Ciencias Políticas*, núm. 111 vol. 39, 2009, pp. 283-304, <https://n9.cl/x9x3o>

⁴⁶ B. SORO MATEO, “Construyendo el principio de precaución”, *Revista Aragonesa de Administración Pública*, núm. 49-50, 2017, pp. 87-151.

No se puede obviar que existen dificultades para trasladar este principio al tema que nos ocupa, ya que la invocación de este principio en las áreas en las que se utiliza, no cabe tan solo por un riesgo percibido, sino precisa de una sólida evidencia científica del mismo⁴⁷. Esta evidencia de carácter científico podría no ser suficiente en cuestiones como la que es objeto de estudio, ya que no parece que el uso de dispositivos conectados a internet sea perjudicial para la salud física de los escolares⁴⁸. En este caso, la cautela habría de ser justificada de acuerdo a otras razones, aunque se han de tener en consideración la multitud de estudios que ponen de relevancia el perjuicio del abuso de las pantallas en el caso de la salud mental. Cabría cuestionarse sobre si es recomendable un uso prolongado de las mismas en horario escolar. En este sentido, en enero de 2023, escuelas públicas de Seattle demandaron a TikTok, Instagram, Facebook, YouTube y Snapchat por los daños mentales que, consideraban, ocasionaban en sus estudiantes y el perjuicio económico que les generaba la necesaria inversión en psicólogos y en capacitar a sus docentes para una atención más especializada⁴⁹.

La profesora Añón ha planteado la necesidad de preservar los derechos humanos, sus garantías y el principio de eficiencia en el uso de modelos algorítmicos de decisión, atendiendo a la inclusión del uso de inteligencia artificial en el marco interpretativo del riesgo o de la prevención de daños a bienes y derechos fundamentales. A su juicio, no se solucionaría la cuestión de la racionalidad decisoria, “aunque vincula las obligaciones orientadas a esta pretensión a una obligación genérica de diligencia debida en el marco de los límites normativos ya existentes relativos a las garantías y protección de los derechos fundamentales”⁵⁰.

⁴⁷ R. SCHOMBERG, “The Precautionary Principle: Its Use Within Hard and Soft Law”, *European Journal of Risk Regulation*, vol. 2, 2012, pp.147-157, https://www.researchgate.net/publication/274716581_The_Precautionary_Principle_Its_Use_Within_Hard_and_Soft_Law

⁴⁸ S. DONGUS et al., “Health effects of WiFi radiation: a review based on systematic quality evaluation”, *Critical Reviews in Environmental Science and Technology*, num. 52 vol. 19, 2022, <https://www.tandfonline.com/doi/full/10.1080/10643389.2021.1951549>. De acuerdo a este reciente y completo estudio, el wifi no afectaría a la salud.

⁴⁹ Estiman que el acceso a internet y el uso de redes sociales ha deteriorado la salud mental de los estudiantes y ampliado el número de trastornos de comportamiento (ansiedad, depresión, trastornos alimenticios y acoso cibernético). Este hecho les ha generado un notable perjuicio económico. V. <https://www.latimes.com/espanol/eeuu/articulo/2023-01-08/seattle-escuelas-demandan-a-redes-sociales-por-salud-mental>

⁵⁰ M. J. AÑÓN ROIG, “Desigualdades algorítmicas: Conductas de alto riesgo para los derechos humanos”, *Derechos y Libertades*, núm. 47, 2022, pp. 17-49.

La cautela o la diligencia debida en el ámbito de los derechos personálísimos, podría justificarse tanto por la necesidad de preservar los derechos de este sector de la población, como por salvaguardar los de los interesados al acceso o rectificación de los datos que se procesan sobre los mismos. No se puede descartar que existe una duda razonable de que estos derechos estén adecuadamente garantizados en ecosistemas en donde un tercero, ajeno a la administración pública, cuenta con la posibilidad de procesar datos en territorio extracomunitario. Estas dudas razonables son de dos tipos. Las primeras se centrarían en los procedimientos iniciados contra Google por abuso de posición dominante. La segunda es la falta de transparencia en la gestión y tratamiento de datos⁵¹.

Las plataformas de software privativo requieren de un registro en sus servidores y la creación de una cuenta y la aceptación en bloque de un contrato de adhesión. El almacenamiento y tratamiento de los datos de los menores estaría vinculado al acceso y contenidos de la dinámica de enseñanza aprendizaje volcados en la plataforma de Google. Existe una salvaguarda de Google en cuanto a que dichos datos no se utilizarán con fines publicitarios, tal y como aparece además en el convenio con la Junta de Andalucía en el 7.10, donde se especifica que la utilización de los datos será “sólo para la finalidad objeto de este encargo”, prohibiendo expresamente su uso para “fines propios ni para la elaboración de perfiles de cualquier tipo”.

Esta previsión o salvaguarda plantea serias dudas si se estudia, incluso someramente, el historial de esta empresa en la UE. Las acusaciones de abuso de posición dominante realizadas en los últimos años debieran producir inquietud en lo referido a su observancia de la legislación vigente. Como ejemplos están las multas que la UE ha impuesto a Google por abuso de posición dominante. Cuantitativamente, es relevante que la UE haya multado en tres ocasiones en dos años y por una cuantía de 8.257 millones de euros. La Comisión Europea multó a Google con 2.424 millones de euros por favorecer a Google Shopping en 2017. En 2019, la Comisión Europea multó a Google con 1.490 millones de euros por prácticas contrarias a la libre competencia en el mercado de la publicidad en buscadores en webs de terceros. Google fue multada en julio de 2018 con 4.343 millones de euros, siendo esta la más alta en la historia de la Comisión. La razón fue sus prácticas anticompetitivas con

⁵¹ Google ha hecho del *contextual advertising* –realizar perfiles de los individuos– una de sus fuentes de beneficio principales; ver J. CHESTER, *The Digital Destiny. New Media and the Future of Democracy*, The New Press, New York, 2007, pp. 144-145.

el sistema operativo para móviles Android. Esta sanción fue confirmada el pasado año por el Tribunal General de la UE en una sentencia de 14 de septiembre de 2022⁵².

Pero también han sido instancias nacionales las que han sancionado a la compañía cuya matriz se denomina Alphabet. Así, en 2020, la Comisión Nacional de Informática y Libertades francesa le impuso una multa de 100 millones de euros –junto con Amazon– por introducir automáticamente, y sin el consentimiento de los usuarios, ‘cookies’ con fines publicitarios. Se trató de una práctica muy grave ya que, incluso cuando el usuario desactivaba la personalización de los anuncios, una de las ‘cookies’ publicitarias continuaba registrando contenidos. Google habría violado la confianza que se establece entre empresa prestadora del servicio y su cliente, en el sentido de que si el último realiza una serie de acciones va a obtener un mayor grado de privacidad. Y no es extraño si pensamos en otros ámbitos de actuación de estas megaempresas en internet. En un reciente estudio sobre libertad de expresión y redes sociales, Valiente Martínez señalaba que “confiar en el buen hacer de los administradores de las redes sociales es arriesgado, pues hasta el momento parecen actuar con opacidad, arbitrariedad y de forma desproporcionada”⁵³.

No solo se han producido estas situaciones en la UE. En *EE.UU.*, el Departamento de Justicia presentó una demanda antimonopolio contra Alphabet por abuso de posición dominante en el mercado en octubre de 2020. Además, estrechamente relacionado con el caso que nos ocupa, Google aceptó pagar una multa de 170 millones dólares en 2019 por almacenar datos de menores, vulnerando la legislación federal y del Estado de Nueva York, vinculado a los vídeos en YouTube. En octubre de 2020, el Fiscal General de Nuevo México acusó a Google de vulnerar la legislación estatal y federal, así como sus propios términos y condiciones de uso del servicio *Google Suite*, de aplicación en las escuelas. En diciembre de 2021, Google aceptó un acuerdo en el que se comprometía a fortalecer la privacidad de niños y adolescentes en su plataforma, que se interpretó como una victoria de la compañía.

En noviembre de 2022, Google aceptó el pago de 391,5 millones de dólares por sus prácticas de seguimiento de ubicación relacionadas con la con-

⁵² <https://curia.europa.eu/juris/document/document.jsf?text=&docid=265421&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=102671>

⁵³ F. VALIENTE MARTÍNEZ, “La libertad de expresión y las redes sociales: de la doctrina de los puertos seguros a la moderación de contenidos”, *Derechos y libertades*, núm. 48, 2023, pp. 167-198.

figuración de la cuenta, que solicitaron los fiscales de cuarenta Estados de Estados Unidos. En este caso, la empresa tecnológica recopilaba datos sobre la ubicación de usuarios, que previamente habían denegado a Google el permiso para que lo hicieran. Según un comunicado de la fiscalía general de Connecticut, Google recopiló información sobre la ubicación de consumidores que expresamente habían pedido que no lo hiciera.

Google es una empresa con ánimo de lucro que responden ante sus accionistas. No existe garantía alguna de uso de los datos con un objetivo comercial. Se menciona que no se utilizarán para un fin publicitario. En los términos y condiciones de uso del servicio, no hay ninguna previsión en cuanto a la minimización o finalidad de los datos procesados o el acceso de los usuarios, cosa que sí sucede en el convenio con la Junta de Andalucía con el fin de cumplir con la legislación sobre protección de datos de la UE. No obstante, ofrece dudas de que Google acepte una previsión, por imposición legal de la UE y de España, que no ofrece con claridad en sus términos y condiciones de uso. Es además de singular significación que los términos y condiciones de uso de esta plataforma sería de una difícil comprensión para aquellos usuarios que no sean juristas o no conozcan la terminología computacional⁵⁴. El contrato de adhesión –es decir los términos y condiciones de uso– establece el texto en idioma inglés como el válido para la interpretación y que será Irlanda, el país donde se resolverán los posibles conflictos. No solo se trata de un cambio de tradición jurídica (derecho continental a *common law*), sino un abierto cuestionamiento del derecho a la tutela judicial efectiva⁵⁵.

La seguridad es crucial en todos los servicios tecnológicos de la sociedad de la información y en las transacciones que se desarrollan⁵⁶. Si se produjera una sustracción de datos en esta plataforma, hecho que no es descartable por

⁵⁴ Se pueden revisar en https://workspace.google.com/terms/dpa_terms.html). En el pliego de contratación de los términos generales aparecen una serie de enlaces dedicados a concretar o ampliar la información contenida en el mismo. Es el caso del punto 6 o del 15. El primero trata de los servicios de asistencia técnica, en el que se contempla el pago de tasas y se especifica que en ciertos casos los “TSS están sujetos a una Tasa mínima periódica, tal y como se describe en la página <https://workspace.google.com/terms/tssg.html>”. En lo que se refiere al 15, se refiere a definiciones de conceptos del contrato que son precisadas en diez enlaces diferentes.

⁵⁵ F. MARTÍNEZ CABEZUDO, “Soberanía tecnológica y gobierno abierto. Profundizando en las necesidades democráticas de la participación desde la tecnopolítica”, *Revista Internacional de Pensamiento Político*, núm. 10, 2015, pp. 66, <https://n9.cl/dhpwd>

⁵⁶ G. GILDER, *Life after Google: The Fall of Big Data and the Rise of the Blockchain Economy*, Regnery Publishing, Washington DC, 2018, p. 7.

la criminalidad que existe en internet, afectaría a menores. Nadie se asombra de las condiciones que existen para aquellos que pretenden poner una guardería infantil o de los controles que desarrolla el Banco de España sobre las entidades de crédito. Son previsiones imprescindibles para garantizar una cierta tranquilidad en el usuario. Se debe ser cauteloso en la custodia y cuidado de niños. Los conciertos en los centros de enseñanza son un buen ejemplo. No es baladí, en consecuencia, cuestionarse la razón de que entidades con ánimo de lucro que operan desde el extranjero, con una infraestructura que se encuentra repartida por el mundo, no se encuentren sujetas a unas garantías más exigentes o bien se les vede, aunque sea de forma cautelar, el acceso a estos datos. Tal y como sucede en el caso de redes sociales y menores, las empresas sitúan el negocio sobre cualquier otro tipo de prioridad como, por otra parte, es lógico en compañías con ánimo de lucro que responden ante sus accionistas. Como señalan Herrera de las Heras y Paños Pérez, ni tan siquiera las plataformas cuentan, en su mayoría, con herramientas que garanticen la veracidad de los datos que ofrece una persona cuando se registra, lo que implica carecer de un método que verifique la edad de los usuarios. Tampoco existe una configuración restrictiva predeterminada para menores con el fin de que el acceso a sus datos tuviera que ser autorizada por ellos o sus progenitores⁵⁷. Lo lógico sería suspender cualquier cooperación hasta no contar con las debidas garantías o mejor, desarrollar herramientas de software libre que permitiera un mayor escrutinio del procesamiento de este tipo de datos personales.

Estas herramientas podrían ser diseñadas por universidades, expertos independientes, la Administración pública o incluso los propios progenitores que deseen implicarse de una forma más activa en la educación de sus hijos. Lo realmente relevante de las mismas sería tanto preservar que los datos permanecen en suelo español, como que la aplicación sea auditable y, por tanto, plenamente transparente y, en consecuencia, de acuerdo con la legislación europea y española en esta materia.

No se debiera rechazar por principio acuerdos con el sector privado para la mejora de la enseñanza y de la infraestructura tecnológica, pero esta colaboración debiera ser siempre extraordinariamente cuidadosa y diligente en la garantía de los derechos de niños y adolescentes. Esta investigación ha tenido como objetivo la detección y análisis de los posibles riesgos e incerti-

⁵⁷ R. HERRERA DE LAS HERAS y A. PAÑOS PÉREZ, *La privacidad de los menores en redes sociales. Especial consideración al fenómeno del Influencer*, Atelier, Barcelona, 2022, p. 66.

dumbres que genera la utilización de plataformas privadas en la enseñanza en el marco de la legislación vigente y en el contexto de los procesos socio-políticos, que influyen en la implementación de las tecnologías de la información en nuestras sociedades. Al establecer la existencia de estos y cernirse una duda razonable sobre su seguridad, se ha planteado el uso de un principio de precaución tecnológica en la escuela respecto a estas plataformas privadas.

Con carácter general, los resultados obtenidos muestran la dificultad de calibrar la entidad del uso que pueden realizar estas plataformas de los datos de los menores. Si bien es cierto que establecen el no uso publicitario de los mismos, es también necesario recordar que no se exceptúa algún otro fin comercial, así como la potencial capacidad de estas empresas de generar productos para estas generaciones. La amplia penetración de estas megaempresas en diferentes mercados hace que puedan obtener una ventaja competitiva gracias a este caudal de datos. La idea de un consumidor atado a un determinado ecosistema tanto como sea posible es un pilar clave del negocio en internet⁵⁸. Tampoco se puede minusvalorar el historial de esta empresa; sus multas y actividades que han provocado preocupación tanto en la UE como en *EE.UU.* Ejemplos como el de Google Street View, donde se violó la privacidad de un buen número de ciudadanos de diferentes países y motivó acciones legales tanto en Europa como *EE.UU.*, calificándose a la aplicación como Google Spy-Fi,⁵⁹ debieran afectar a su credibilidad⁶⁰.

La relación entre Administración y administrado en el marco de un servicio público, gratuito y universal es muy diferente que el vínculo contractual que se establece con un particular. El alumnado y sus padres o tutores desconocen el alcance de los datos que son transferidos. La falta de una educación sobre internet, tanto para unos como para otros, hace que no se comprendan las implicaciones de este tipo de relación contractual o se minimicen los efectos. Los hechos parecen desmentir la idea de “nativo digital”. Así, para algunos expertos, lo que tenemos son huérfanos digitales, “que muestran

⁵⁸ R. W. MCCHESENEY, *Digital Disconnect. How Capitalism is Turning the Internet Against Democracy*, The New Press, New York, 2013, p. 140.

⁵⁹ S. ZUBOFF, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Profile Books, London, 2019, p. 144.

⁶⁰ También ha trascendido el caso de TikTok. Gracias a la legislación europea en materia de protección de datos, se supo que algunos de sus trabajadores podían acceder a los datos de los usuarios en remoto. La Comisión y el Consejo de la UE han prohibido el uso de TikTok en los dispositivos electrónicos de sus funcionarios.

una preocupante falta de formación incluso en los niveles más básicos”⁶¹. La generación de los ochenta podía contar en sus institutos de bachillerato con asignaturas de programación en Basic, sin tener en cuenta si eran de ciencias o letras. Hoy en día, hasta esa enseñanza parece haber quedado sustituida por un uso de aplicaciones cerradas. Los adultos tampoco parecen estar mejor preparados, probablemente, porque nadie se ha preocupado de formarlos. Resulta urgente un replanteamiento del uso y aprendizaje de las nuevas tecnologías en la escuela para que el alumnado no sea sujeto pasivo de la revolución tecnológica en la que nos encontramos.

4. CONCLUSIONES

Hay dos cuestiones que se deben tener en consideración después del análisis realizado. En primer lugar, debiera reivindicarse una formación específica sobre internet. La educación sobre internet es tan relevante como a través de internet. Los estudiantes han de comprender las posibilidades de la Red, pero también estar alerta para proteger sus derechos, además de prestar atención a sus deberes. Esta formación ayudaría a preservar bienes jurídicos decisivos tanto en el espacio virtual como no virtual. Sin este tipo de formación, no se da la importancia que merece a cesiones de datos o firmas de contratos de adhesión con cláusulas discutibles.

En segundo lugar, la introducción de un principio de precaución tecnológica posibilitaría una gestión responsable de nuestra privacidad, en cooperación con las Administraciones públicas. Ante situaciones de incertidumbre, establece límites a la acción de entes privados con ánimo de lucro y genera una reflexión sobre la necesidad de articular vías alternativas. Las empresas privadas pueden proveer de soluciones que facilitan el derecho a la educación y reduzcan posibles brechas en la administración de este servicio, pero todo ello se debe llevar a cabo desde el respeto de los derechos fundamentales. El que se trate de algo que está en la web y que parece evanescente, no debería servir para menospreciar o minusvalorar su impacto. Esta conclusión es extrapolable a cualquier plataforma similar de otra empresa privada. En relación a las compañías transnacionales que gestionan datos personales, se debe tener en cuenta que es de singular importancia vigilar si salen del territorio de la UE.

⁶¹ E. DANS, “Prólogo: Los nativos digitales no existen”, en S. LLUNA y J. PEDREIRA, *Cómo educar a tus hijos para un mundo digital*, Deusto, Barcelona, 2017, p. 25.

En el caso del tratamiento de los datos personales del sector poblacional objeto de este estudio, como en el del medio ambiente, la seguridad alimentaria o los productos químicos, se debe ser singularmente exigente. Sus datos son muy valiosos y conforman su identidad y personalidad. Que una empresa privada extranjera tenga acceso a ellos y los procese durante años, sin que exista la completa seguridad de que no se abre una vía para la vulneración de bienes jurídicos básicos debería ser razón suficiente para la cautela. La falta de claridad, vaguedad o incertidumbre en su custodia supone un verdadero desafío para nuestras sociedades. De los resultados obtenidos se desprenden tres conclusiones.

La primera es que los datos son uno de los recursos más valiosos que existen en la actualidad. Su almacenamiento y tratamiento han de quedar sometidos a legislaciones muy garantistas. En segundo lugar, la escuela se configura como un centro de educación y formación cívica que debe incorporar en su praxis un uso responsable de internet. Esta utilización pasa por tomar en serio el vínculo que se establece entre alumnado, plataformas y administración pública. En tercer lugar, existen suficientes elementos para establecer un principio de cautela tecnológica, en analogía con el derecho ambiental, la legislación sobre seguridad alimentaria o el uso de sustancias químicas, que evalúe con rigor y sin prisas la situación, con el fin de limitar los efectos indeseados de la incertidumbre generada alrededor de la utilización que las empresas privadas puedan realizar de los datos de los menores. Si la administración educativa establece límites y exigencias a las entidades que desean ser parte de la enseñanza concertada, no se entiende que no se aprecie un modelo similar con respecto a la enseñanza dentro del aula. Si los titulares de la patria potestad tienen limitado el acceso a los contenidos que producen sus hijos y, por tanto, a su vida online, no se comprende que no se sea exigente con una entidad ajena a las familias y a la Administración pública.

En definitiva, se puede concluir que se ha de ser cauteloso con el uso de plataformas de empresas privadas en el entorno escolar. Esta precaución se justifica por una serie de indicios que generan relevantes dosis de incertidumbre respecto al tratamiento y custodia de los datos que realizan estas corporaciones y se traduce en la necesidad de obtener más garantías, lo que probablemente tenga como consecuencia el desarrollo de legislaciones más garantistas.

Esta investigación tiene varias limitaciones. Aun no contamos con informes sobre el uso de la plataforma objeto de estudio en la escuela y la ex-

perencia concreta que se ha tenido en las aulas. Este hecho se traduce en que carecemos de una información contrastada sobre sus ventajas e inconvenientes desde el plano pedagógico, al ser una plataforma de reciente creación. Tampoco existen en Europa investigaciones, como las desarrolladas en *EE.UU.*, respecto a los datos recabados por esta plataforma. Desconocemos si las prácticas que han motivado la actuación de las autoridades estadounidenses se han llevado a cabo en Europa, aunque pueden haber indicios de que se ha replicado un comportamiento semejante. Por ejemplo, en Francia se prohibió en las escuelas e institutos el uso de las versiones gratuitas de Google Workspace for Education por la presunta vulneración de la regulación europea de protección de datos.

En cuanto a futuras líneas de investigación, referidas a los análisis realizados centrados en el uso de plataformas de software privativo en educación, sería necesario estudiar otras similares, como la de Microsoft, a fin de establecer semejanzas y paralelismos. Otra posibilidad es que se desarrollen plataformas libres y eficaces que respondan a las necesidades de enseñantes y estudiantes. En este caso, se trataría de reflexionar sobre sus ventajas e inconvenientes respecto a plataformas como *Google Workplace for Education*.

Todas las páginas web con acceso el 14/04/2023

RAFAEL RODRÍGUEZ PRIETO
Universidad Pablo de Olavide
Carretera de Utrera km.1
41013, Sevilla
e-mail: rrodpri@upo.es