Leer, jugar, aprender y comunicarse en un entorno seguro: seguridad, privacidad y confidencialidad en las aplicaciones infantiles

Read, play, learn and communicate in a safe environment: security, privacy and confidentiality in children's applications

Raquel Gómez-Díaz; **Araceli García-Rodríguez**

Gómez-Díaz, Raquel; **García-Rodríguez, Araceli** (2020). "Leer, jugar, aprender y comunicarse en un entorno seguro: seguridad, privacidad y confidencialidad en las aplicaciones infantiles". *Anuario ThinkEPI*, v. 14, e14c02.

https://doi.org/10.3145/thinkepi.2020.e14c02

Publicado en *IweTel* el 11 de junio de 2020

Raquel Gómez-García

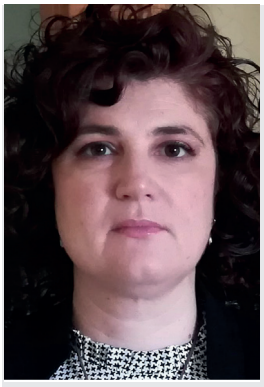
https://orcid.org/0000-0002-1423-1315

Universidad de Salamanca
Grupo E-Lectra
Facultad de Traducción y Documentación
Francisco de Vitoria 6-16. 37008 Salamanca, España
rgomez@usal.es

Araceli García-Rodríguez

https://orcid.org/0000-0003-4102-3340

Universidad de Salamanca
Grupo E-Lectra
Facultad de Traducción y Documentación
Francisco de Vitoria, 6-16. 37008, Salamanca, España
araceli@usal.es



Resumen: La preocupación generalizada por proteger la privacidad, seguridad y confidencialidad de los menores en el entorno digital ha propiciado la aprobación de leyes nacionales e internacionales, la incorporación de artículos específicos en la legislación existente y la creación de sellos de calidad que tratan de evitar la recopilación y el uso inadecuado de los datos. En estas normativas, se exige, entre otras cosas, que se redacte una política de privacidad y seguridad clara y concisa, que sea pública, transparente y conocida por los usuarios. Es necesario conocer si las empresas incluyen este tipo de información en las aplicaciones o sus webs, y sobre todo qué datos deben aparecer. Solo de esta forma los adultos podrán hacer un uso adecuado de dicha información de cara a permitir la descarga y uso de esas aplicaciones por parte de los menores.

Palabras clave: Políticas de seguridad; Privacidad y confidencialidad; Aplicaciones infantiles; Legislación; Normativa.

Abstract: The widespread concern to protect the privacy, security and confidentiality of minors in the digital field has led to the approval of national and international laws, the incorporation of specific articles in existing ones and the creation of quality seals, trying to avoid the collection and inappropriate use of data. This regulation requires, among other things, that developers write a clear and concise privacy and security policy, that it be public, transparent and known to users. It is necessary to know if companies include this type of information in applications or their websites, and especially what data should appear. Only in this way adults will be able to decide or nor to allow the download and use of these applications by minors.

Keywords: Security; Privacy; Confidentiality; Policies; Children's apps; Regulations; Legislation.

1. Introducción

Según el *Informe de medios digitales* del *PwC* de 2019 (*PwC*, 2019) en 2018 el 40% de los usuarios de internet en el mundo eran niños. Este grupo de edad constituye la audiencia que más ha crecido en la Red en los últimos años y en la actualidad son millones los que utilizan o acceden a todo tipo de contenidos digitales, entre ellos aplicaciones para dispositivos móviles.

La incorporación de la tecnología es imparable y cada vez son más los menores que tienen contacto con ella a una edad más temprana, por lo que es prioritario garantizar que estos se muevan en entornos seguros, en el denominado espacio *Kidtech*.

Esta incorporación al consumo de contenidos digitales por parte de los menores ha ido acompañada de una preocupación por su seguridad digital, por garantizar un acceso seguro de "cero datos" para programadores y marcas (figura 1). Hay que tener en cuenta que inicialmente el consumo digital no fue diseñado para ellos, por lo que es necesario contar con medidas que limiten la exposición a contenidos no aptos, a publicidad intrusiva y poco adecuada y a evitar que se incumplan los requisitos básicos de privacidad (derecho a decidir qué datos personales se quiere compartir y cuáles no), confidencialidad (acceso a información por parte únicamente de las personas autorizadas [ISO/IEC 27002:2013] o protección de datos) y seguridad, aludiendo en este caso al acceso a contenidos no adecuados, a compras integradas, o publicidad intrusiva. De hecho, la Comisión Europea tipificó ya en 2006 los principales riesgos para los menores, entre los cuales están los asociados al contacto con desconocidos, los relacionados con los contenidos inapropiados y los relativos a la privacidad (**Crescenzi-Lanna**; **Valente**; **Suárez-Gómez**, 2019).

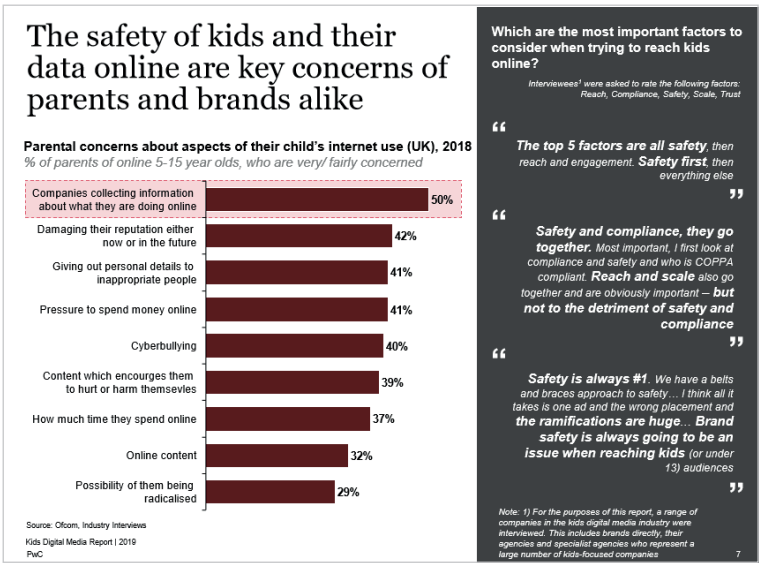


Figura 1. Preocupaciones de los padres sobre el uso de internet por parte de los niños
https://content.superawesome.com/pwc-kids-digital-advertising-report-2019

La preocupación generalizada por proteger la privacidad, seguridad y confidencialidad en el ámbito digital es una constante por parte de los padres (figura 1), que, a nivel institucional, ha dado lugar a la aprobación de leyes, a la incorporación de artículos específicos en la legislación existente y a normas que regulan la publicidad ilegal para público infantil, cookies y plugins, verificación de edad, consentimiento informado de padres, etc.

Estados Unidos fue el país pionero en lo relativo a la protección de datos de los menores con la *Children's online privacy protection act* (*Coppa*). Una ley federal de la *Asociación Federal de Consumidores de Estados Unidos* (*FTC*), que, aunque aprobada en 1998, no entró en vigor hasta el año 2000. Esta ley regula la forma en la que apps, juegos y sitios web están autorizados para recopilar y procesar información personal de los menores de 13 años.
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Los aspectos principales recogidos en la *Ley Coppa* se pueden resumir en los siguientes (*Levanta la cabeza*, 2019):

- Obligación del consentimiento informado de los padres para la recopilación de datos de menores: dirección, e-mail, teléfono, imagen, grabación de voz, localizador e identificador de dispositivo.
- Prohibición del uso de la geolocalización o cualquier otra tecnología de seguimiento de dispositivos.
- Imposibilidad de realizar envíos de publicidad personalizada a partir de datos obtenidos mediante cookies o basándose en su comportamiento.

"La Covid-19 había logrado abrir un resquicio en la fortaleza de la propiedad intelectual y los derechos de autor contemplados desde la óptica más rígida"

- Alcance extraterritorial: se aplica a empresas infractoras que estén fuera de los Estados Unidos y a empresas de Estados Unidos, aunque el consumidor del contenido no sea de este país.
- A partir de 2013, obligación por parte de los operadores de hacer pública la política de privacidad, indicando claramente los datos recopilados.

Esta ley general se completó en el año 2000 con la *Children's internet protection act* (*Cipa*), sobre contenidos no adecuados en internet en bibliotecas y centros educativos que reciben descuentos mediante el programa *E-rate*[1]. Estos centros deben certificar la utilización de medidas de protección tecnológica (filtros) y tareas de formación, para impedir el acceso a determinados contenidos perjudiciales para los menores. Ver guía de los consumidores en:
https://www.fcc.gov/sites/default/files/childrens_internet_protection_act_cipa.pdf

Por su parte, en 2016 la Unión Europea, el *Parlamento* y el *Consejo Europeo*, aprobaron el *Reglamento 2016/679/CE 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* (*Unión Europea*, 2016), de obligado cumplimiento a partir del 25 de mayo de 2018, que regula el procesamiento por un individuo, una empresa o una organización de los datos relativos a personas en la UE y afecta a todos los europeos, aunque los datos sean recogidos por empresas de otros países.

En el artículo 8 del Reglamento se indican las "Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información", y se establece que los niños son población vulnerable que necesita protección específica, determinando que el tratamiento de la información personal de un menor se considerará lícito a partir de los 16 años; con menos de esta edad, el tratamiento solo se considera lícito si se da el consentimiento del titular de la patria potestad o el tutor, si bien da libertad a los Estados miembros para establecer por ley una edad inferior, nunca menor de 13 años.

"Es necesario que los programadores redacten una política de privacidad y seguridad clara y concisa y que esta sea pública, transparente y conocida por los usuarios"

Esta consideración como personas vulnerables, obliga a que se proteja su desarrollo emocional, integridad moral y dignidad, según explica Alicia Piña, coordinadora de la Comisión de Menores de la *Asociación Profesional Española de Privacidad* (*APEP*) (**Rubio**, 2018) y al igual que en la ley americana, requiere que los programadores informen a los niños y a sus padres sobre el tratamiento de sus datos personales en un lenguaje "claro, sencillo y fácil de entender para su edad".
https://www.apep.es/?v=3b0903ff8db1

En España, en diciembre del 2018 se aprobó la *Ley Orgánica 3/2018 de protección de datos personales y garantía de los derechos digitales* para adaptar el ordenamiento jurídico español a la normativa europea antes mencionada (*España*, 2018). En el artículo 7 titulado *Consentimiento de los menores de edad*, se establece que en lo relativo al tratamiento de datos personales solo puede dar directamente su consentimiento cuando sea mayor de 14 años[2].

Al mismo tiempo que se han ido promulgando las distintas leyes se está observando un mayor celo en la vigilancia de su aplicación y una mayor presión contra los que la infringen. Prueba de ello es, por ejemplo, la multa de 170 millones de euros impuesta a *Youtube* por incumplir la *Ley Coppa*, al recopilar y utilizar datos e información de menores de 13 años para fines comerciales, imponiéndole la obligación de limitar la forma en la que recopilan los datos de menores y la prohibición de mostrar anuncios personalizados con los datos obtenidos sobre sus hábitos y actitudes (**Hatch**, 2020).

Esta preocupación se observa también en diferentes iniciativas. En el ámbito público se puede mencionar:

- creación, por parte de 27 autoridades responsables de hacer cumplir la normativa de privacidad, de la *Global Privacy Enforcement Network* (*GPEN*)
  https://www.privacyenforcement.net
- *International Privacy Law Library*, una red de institutos de información legal que cooperan con el *World Legal Information Institute*
  http://www.worldlii.org/int/special/privacy

Destacar también la creación en el Reino Unido en 2018 del *Age Appropriate Desing Code* (AADC), un conjunto de pautas de diseño para que los servicios digitales infantiles cumplan la ley europea, y que amplía la protección hasta los 18 años.
https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services

Asimismo, se han creado sellos de calidad y seguridad para garantizar que los productos cumplen la *Ley Coppa*, como:

- *Kids Safe Certified*
  http://www.kidsafeseal.com
- *Parent's Choice Awards*
  https://www.parentschoice.org

En el ámbito privado, las tiendas de aplicaciones han incluido secciones específicas para niños o familias (*Kids* en *Appstore* o *Familia* en *Google*) para que los programadores incorporen productos seguros para niños. Por otro lado, están surgiendo empresas especializadas en ofrecer servicios a los programadores para la creación de contenidos para niños que cumplan con la legislación vigente. Es el caso de *Superawesome*, una empresa de publicidad especializada en la creación de contenido para menores, que ha lanzado su *Kids web services*. Su servicio se basa en diferentes funcionalidades con tecnología para niños (*kidtech*) que hacen tareas automáticas de autentificación segura. Se incorpora además un sistema de fidelización a través de estrategias de gamificación que permiten al usuario conseguir puntos para desbloquear contenidos mediante la interacción con el sitio web o app (**Yuste**, 2016).
https://www.superawesome.com

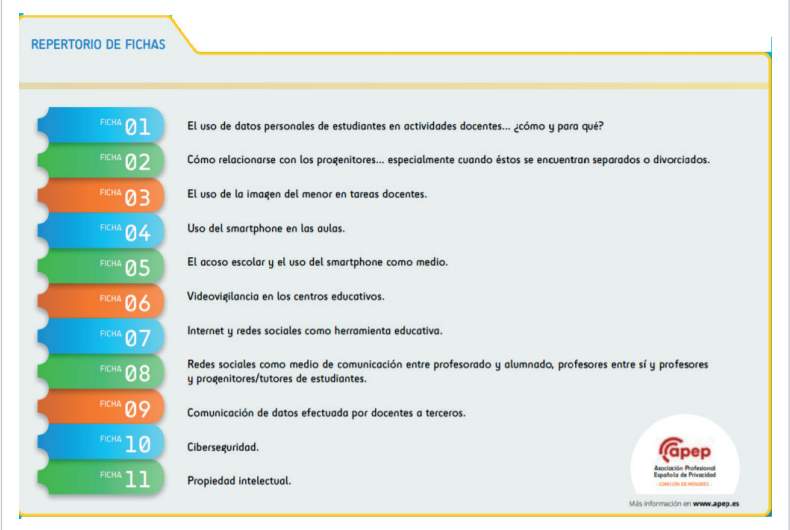


Figura 2. Ejemplo de ficha elaborada por APEP
https://www.apep.es/wp-content/uploads/2020/01/Fichas-Privacidad.pdf?v=3b0903ff8db1

En España, la *Asociación Profesional Española de Privacidad* (*APEP*) ha creado una *Comisión de Menores*, desde la que se organizan jornadas y cursos, y que participa en grupos de expertos como la entidad pública estatal *Red.es* o el *Congreso de los Diputados*. Ha elaborado diferentes fichas de trabajo con consejos y orientaciones dirigidas al ámbito escolar
https://www.apep.es/wp-content/uploads/2020/01/Fichas-Privacidad.pdf?v=3b0903ff8db1

En toda la legislación mencionada, se hace hincapié en la necesidad de que los programadores redacten una política de privacidad y seguridad clara y concisa y que esta sea pública, transparente y conocida por los usuarios, una recomendación que es aplicable a todo tipo de contenidos digitales, incluidas las apps en las que nos centramos en este artículo.

2. ¿Qué ocurre con las apps?

Al igual que con otros formatos digitales, cada vez es mayor el tiempo que los niños pasan leyendo, aprendiendo, comunicándose o jugando con una app y es necesario ser conscientes de que estas también pueden recopilar y compartir información personal, permitir compras integradas, facilitar el acceso a redes sociales o incluir publicidad no adecuada, tal y como se muestra en la figura 3.

Es importante ser conscientes de que muchas apps para móviles y tabletas pueden conocer en todo momento dónde está el menor, utilizar la cámara o el micrófono para grabar sus reacciones cuando está interactuando con el dispositivo, y compartir todo esto con terceros; una información muy útil para los programadores, interesados en recabar datos directos de los demandantes de contenidos: gustos de navegación, ubicación, tiempo de conexión, tipos de contenidos, etc. son datos especialmente interesantes, ya que permiten

> "obtener un perfil exacto de los menores porque ellos son los próximos demandantes de contenidos y aplicaciones" (**Rubio**, 2018).

Diferentes investigaciones han demostrado que la legislación sobre protección de datos no siempre se cumple en las apps dirigidas a menores.

Así, por ejemplo, los investigadores del *Computer Science Institute* de la *Universidad de Berkeley* estudiaron el comportamiento, en tiempo real, de unas 6.000 apps infantiles de *Android* disponibles en la tienda de Estados Unidos. Dicho estudio permitió conocer con qué frecuencia y bajo qué circunstancias se obtenían datos confidenciales y a dónde se enviaban, y gracias al monitoreo de las aplicaciones agilizar la información sobre el cumplimiento de la *Ley Coppa*. Los resultados de este trabajo revelan

que más de la mitad de las aplicaciones estudiadas cometía algún tipo de infracción, pero además sirve de banco de pruebas para que los programadores puedan evaluar el grado de cumplimiento de las políticas de privacidad y requisitos reglamentarios, antes de lanzar esas aplicaciones al público ya que muchas de las dificultades se deben a los programas SKD (*Kit de desarrollo de software*)[3] que implementan en sus aplicaciones (**Reyes** *et al.*, 2018).

Un artículo publicado en 2018, en *The New York Times* (**Valentino-Devries**, et al., 2018), también se hacía eco de la demanda a un programador de una app (*Fun Kid Racing* de *Tiny Lab Productions*) dirigida a niños, por recopilar datos y ubicación, pese a estar en la sección familiar de *Google*, en la que se supone que los contenidos cumplen todos los requisitos de seguridad. Los autores del artículo analizaron veinte de las aplicaciones infantiles de *iOS* y *Android* y comprobaron que, especialmente en la categoría "juegos", pese a someterse a los filtros de control parental de las tiendas y dispositivos, se recogían datos de localización, contacto o características demográficas. La multinacional *Disney* fue demandada igualmente por comercializar 42 aplicaciones para niños que recogían datos de menores con el objetivo de crear perfiles para anuncios personalizados.

Por otro lado, según un informe de *Global Privacy Enforcement Network*, el 41% de las apps y web de los 1.500 productos analizados presenta algún aspecto preocupante:

- 67% recopila datos personales, sobre todo nombres y correos;
- 50% comparte datos con terceros;
- 22% les pide su número de teléfono;
- 23% les permite compartir fotos y vídeos.

Figura 3. Información que puede recopilar una app
https://www.consumidor.ftc.gov/articulos/s0351-infografica-de-aplicaciones-para-ninos

Además, advierte que el 31% carece de controles que limiten la recolección de datos de los menores. El 71% de las apps y páginas web analizadas pone las cosas muy difíciles al progenitor si decide eliminar la cuenta o parte de los datos personales que el menor haya introducido previamente. Solo el 24% promueve la participación de los padres a través de control parental, avatares o la creación perfiles de usuarios diferentes. Esto no quiere decir que estas infracciones sean intencionadas, tal como indica uno de los autores del informe, afirmando que

> "Lo más probable es que estén causadas por descuidos al incluir software de terceros [SDK] en las aplicaciones" (**Gonzalo,** 2018).

3. ¿Qué hay que incluir en una política de privacidad de una app?

Es evidente que, además del tiempo de exposición a las pantallas, seguridad, confidencialidad y privacidad son temas que preocupan, por lo que cada vez es más importante que los adultos conozcan la legislación vigente sobre protección de datos, las herramientas de seguridad de las apps, dónde se especifica la política de privacidad de los programadores y qué información debe incluir.

Aunque no es una práctica habitual, es muy recomendable que los adultos lean con detenimiento la política de privacidad de una app infantil antes de descargarla, conociendo previamente aquellos puntos que deben aparecer claramente especificados y que recogemos a continuación, con la idea de, en un trabajo posterior, utilizarlos como parámetros de análisis y aplicarlos al estudio de las políticas de los programadores.

1) Seguridad

Cuando hablamos de seguridad, nos referimos básicamente al control parental, a todas las acciones encaminadas a la protección de los menores respecto del uso que hacen de la tecnología (**García-Rodríguez**; **Gómez-Díaz**, 2016, p. 22). A pesar de que las tabletas cuentan con sistemas de control específicos, en aquellos productos que permitan acceso a internet o compras integradas, es necesario que exista una acción de control propia y adecuada a la edad de los destinatarios, o bien que estas acciones solo se puedan realizar desde una sección limitada a los adultos (**Gómez-Díaz**; **García-Rodríguez**, 2018).

"Es recomendable que los adultos lean con detenimiento la política de privacidad y seguridad de una app infantil antes de descargarla"

El control parental se puede realizar de tres maneras distintas: en el dispositivo, sobre las apps o instalando una app de terceros que haga estas funciones. En este caso solo es responsabilidad del programador incluirla en la propia app para impedir el acceso a las compras, a redes sociales o a contenidos complementarios destinados a los padres. Requiere de la realización de una acción por parte del menor, por ejemplo, una operación matemática, o escribir algo. Lo importante es que la acción no sea fácilmente descifrable para los menores a los que esté destinada.

Dentro de las apps es necesario mencionar aquellas que cuentan con versiones especiales para niños, en este caso, aunque mantengan parte del diseño este es más sencillo y sobre todo el control parental viene activado de fábrica. Es el caso de *YouTube Kid*s o de *Netflix*, donde el perfil infantil tiene sistemas de búsqueda de contenidos adaptados a los menores.

En el caso de las apps lo que hay que comprobar es:

- Existencia o no de sistema de control parental dentro de la app.
- Tipo de control: redes sociales, compras integradas, tiempo de uso…
- Sistema de desbloqueo adecuado o no a la edad para la que está recomendada la app.

2) Privacidad y confidencialidad

Para cumplir tanto con la legislación europea (*Unión Europea*, 2016, artículo 12), como con la española (*España*, 2018, artículo 11), un programador de apps debe seguir una política de transparencia en lo que se refiere a la recogida, tratamiento y uso de los datos y la obligación de notificarla con un lenguaje claro y sencillo que sea comprensible por niños, una información que debe ser facilitada en todo tipo de medios, impresos y electrónicos. Siguiendo esta premisa se deberán tener en cuenta los siguientes aspectos.

2.1) Disponibilidad de la información

a. En la web del desarrollador en un sitio visible. Es habitual que esta información se incluya al final de la página y en letra pequeña que pasa totalmente desapercibida. Sería recomendable que apareciera en las pestañas destacadas de la primera página.
b. En la tienda con un enlace directo o como mínimo a la app del programador, incluyendo siempre enlaces activos.
c. En la propia app.

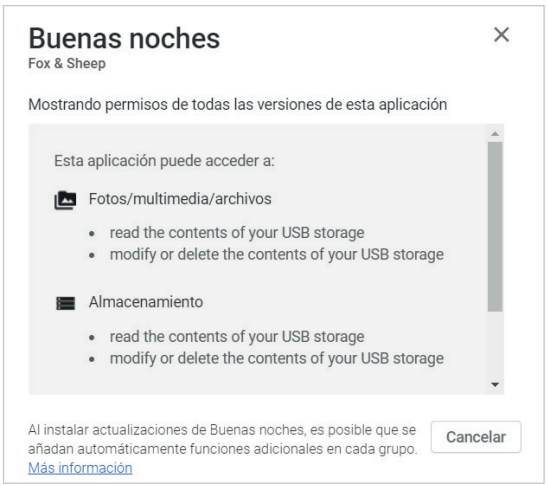


Figura 4 Ejemplo de disponibilidad de la información en la tienda app "Buenas Noches" (*Fox & Sheep*)
https://play.google.com/store/apps/details?id=-com.foxandsheep.nightynight&gl=ES

2.2) Información general

a. Especificación de la ley que afecta a la app y el ámbito geográfico.
b. Vigencia de la política de privacidad incluyendo la fecha de la última revisión.
c. Sistema de información a los usuarios en caso de cambios, aviso personal, lista de distribución, boletín informativo...

2.3) Información recopilada

a. Declaración expresa de no recopilar datos de menores.
b. Si se recogen ciertos datos de menores, indicación clara e inequívoca de la autorización paternal,

indicando la edad considerada en función de la normativa aplicada, 13, 14 o 16 años.

c. Datos personales recogidos, tanto de adultos como de niños: e-mail, nombre, teléfono, etc.

d. Datos de uso que se recaban de forma automática: tiempo de uso, pantallas vistas, tipo de navegador y sistema operativo e interacciones realizadas, suelen ser los habituales.

e. Datos analíticos de terceros. Se incluyen en esta categoría empresas que elaboran servicios para aplicaciones, analítica, integración con redes sociales y monetización a través de anuncios. Estas reciben un flujo constante de datos tanto a través del navegador como de las apps y tienen la capacidad de hacer un seguimiento de los usuarios sin su conocimiento. Se debe indicar qué servicios o proveedores se utilizan para ello y si se requiere autorización explícita.

"Un programador de apps debe seguir una política de transparencia en lo que se refiere a la recogida, tratamiento y uso de los datos, pero también notificarla con un lenguaje claro y sencillo que sea comprensible por niños"

2.4) Uso de la información

Las compañías están obligadas a exponer el tratamiento que se va a dar a los datos con indicación de autorización expresa para cada una de las finalidades.

a. Declaración del uso de los datos: mejorar la app, enviar publicidad de sus productos…

b. Indicación de si comparten o no datos con otras compañías. Las apps pueden compartir los datos recopilados con sus proveedores y empresas afiliadas para entender cómo los usuarios usan el servicio y mejorarlo, como ocurre con la app *myABCKit: aprender a leer* (Aprender jugando) donde se especifica "Utilizamos los datos que tenemos sobre ti para proporcionar y personalizar nuestros servicios".

c. Uso de cookies y durante cuánto tiempo se utilizan.

2.5) Almacenamiento de datos

Se informará al usuario, del plazo durante el cual se conservarán los datos personales y los criterios utilizados para determinar este plazo.

2.6) Compras dentro de la app

Este dato debe estar claramente especificado en la tienda, pero también es conveniente indicarlo en la política de privacidad, informando además sobre la forma en la que está protegida la compra.

2.7) Publicidad

Es necesario indicar si la incorporan o no y en caso de incluirla, si es solo de sus productos o también de terceros. Lo más recomendable es que disponga de un boletín mediante el cual el usuario pueda o no dar su conformidad para recibir publicidad. También es interesante que indique si se utilizan redes de publicidad seguras.

2.8) Redes sociales

Indicar si se permite acceder o no desde la app y el sistema de control para que solo lo hagan adultos.

2.9) Derechos

Rectificación, eliminación, recursos, etc. en función de la ley aplicable en cada caso.

Figura 5. Presentación de la información del programador *Chiquimedia*
https://chiquimedia.org/es/apps/nurot/child-safety

2.10) Presentación de la información

Los textos deben ser claros, entendibles y sencillos y estar traducidos al idioma del usuario de la app.

4. Conclusiones

Como afirma **Falestchi**, (2020) es fundamental crear un ecosistema digital seguro y relevante para niños que garantice experiencias innovadoras y entretenidas, a través de herramientas que potencien marcas y creadores de contenidos. Para ello es fundamental, no solo la existencia de leyes, sino

también, teniendo en cuenta que las aplicaciones están disponibles en tiendas de diferentes áreas geográficas, que estas sean lo más uniforme posible en lo relativo a la recogida y uso de datos, y especialmente a la edad considerada como mínima para el consentimiento parental. Si bien la edad que se contempla es hasta los 13 (Estados Unidos y algunos países europeos) o incluso 14 (España) es conveniente ampliar el concepto de menores hasta los 16 años tal y como expresan **Krivokapic y Adamovic** (2016). Estamos ante un panorama legal que cambia rápidamente, que requiere que las compañías que operan en el espacio de los niños se vean obligadas a mantenerse constantemente actualizadas.

"Las nuevas generaciones ya nacen con una huella digital provocada por los datos que se van recolectando y por los datos que de ellos suben padres y familiares, muchas veces por desconocimiento o negligencia"

Cada vez es más importante la responsabilidad de los adultos en lo que a la lectura y revisión de la política de privacidad se refiere. Por ello es imprescindible que sean los padres quienes controlen qué aplicaciones descargan los niños y se involucren en el uso que les dan, que utilicen herramientas efectivas de control parental y especialmente que lean y comprueben la política de privacidad antes de descargarlas. Juan Pablo Peñarrubia, vicepresidente del *Consejo General de Colegios Profesionales de Ingeniería Informática* (*CCII*), subraya el riesgo al que se exponen los menores al utilizar apps por su "falta de criterio y conciencia":

> "Un menor no tiene la formación, ni sobre todo el sentido común y la experiencia para tener un comportamiento adecuadamente prudente en relación con internet y los servicios digitales".

La percepción de los niños, sostiene, es que

> "el servicio es así de modo natural y que si hubiera algo ilegal estaría prohibido: Si para un adulto ya es difícil resistirse al 'aceptar, aceptar, aceptar...' de las apps, para un menor es aún más complicado" (**Rubio**, 2018).

Es un gran avance que se haya legislado sobre el control y la seguridad de los menores, que se haga un seguimiento de las actividades de los programadores y que se sancionen las malas prácticas, pero la responsabilidad última de los adultos proteger y asegurar que nuestros niños están en un entorno garantizado.

Esto supone que también se obligue a los programadores a que redacten las políticas de forma clara y comprensible, incorporando toda la información anteriormente mencionada, así como diseñando herramientas o instrumentos que permitan confirmar, inequívocamente, que es un adulto el que está autorizando la recogida de datos, en caso de que se haga, así como para verificar qué se está haciendo con los datos que se comparten con terceros. Las tiendas de apps pueden ejercer presión al respecto, comprobando que efectivamente la política de privacidad de un programador cumple con los requisitos, antes de autorizar la incorporación de sus productos al catálogo.

"El problema de raíz es que se ha portado un modelo de negocio diseñado para adultos a las aplicaciones de menores"

Las nuevas generaciones ya nacen con una huella digital provocada por los datos que se van recolectando y por los datos que de ellos suben padres y familiares, muchas veces por desconocimiento o negligencia (**Gonzalo**, 2018). Como afirman los expertos, si resulta complicado para un adulto controlar los diferentes aspectos relacionados con la privacidad y seguridad, mucho más para los menores, por eso la definición, difusión y conocimiento de estas políticas pueden ser un primer paso.

Según Vallina (investigador del *IMDEA Networks* de Madrid) (**Gonzalo**, 2018), será muy interesante ver qué pasa con el nuevo reglamento europeo en relación con los trackers (rastreadores) de datos.

> "El problema de raíz es que se ha portado un modelo de negocio diseñado para adultos a las aplicaciones de menores. Quizás deberían buscar otro modelo más respetuoso con los niños"

5. Notas

1. *E-rate* es un programa que proporciona descuentos en acceso a internet y telecomunicaciones en colegios y bibliotecas, especialmente en zonas rurales.
https://www.usac.org/e-rate/

2. Es probable que la edad se rebaje a los 13 años como aparece recogido en el anteproyecto de ley para desarrollar el reglamento comunitario.

3. Conjunto de herramientas de desarrollo de software que permite a un desarrollador de software crear una aplicación informática para un sistema concreto

6. Referencias

Children's internet protection Act (*Cipa*): *Guide.*
https://www.fcc.gov/sites/default/files/childrens_internet_protection_act_cipa.pdf

Children's internet protection Act (*Cipa*): Consumer
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Children's online privacy protection act (*Coppa*).
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Crescenzi-Lanna, L.; **Valente, Riccardo**; **Suárez-Gómez, Rafael** (2019). "Aplicaciones educativas seguras e inclusivas: La protección digital desde una perspectiva ética y crítica". *Comunicar*, v. XXVII, n. 61, p. 93-102.
https://doi.org/10.3916/C61-2019-08

España (2018). "Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales". *BOE*, n. 294, 6 diciembre.
https://www.boe.es/eli/es/lo/2018/12/05/3

Falestchi, Demian (2020) "Cómo se protege a los niños en internet en 2020" *Infobae*, 3 febrero.
https://www.infobae.com/america/opinion/2020/02/03/como-se-protege-a-los-ninos-en-internet-en-2020

García Rodríguez, Araceli; **Gómez-Díaz, Raquel** (2016). *Lectura digital infantil: dispositivos, aplicaciones y contenidos*. Barcelona: Editorial UOC. Colección El profesional de la información, n. 33. ISBN: 978 84 9116 433 3

Gómez-Díaz, Raquel; **García-Rodríguez, Araceli** (2018). "Criterios de calidad y estándares de presentación en los libros-app: el sector de los contenidos infantiles". *El profesional de la información*, v. 27, n. 3, pp. 595-603.
https://doi.org/10.3145/epi.2018.may.12

Gonzalo, Marilín (2018) "Más de la mitad de las aplicaciones infantiles envía datos a terceros". *El país*, 7 mayo.
https://elpais.com/tecnologia/2018/04/30/actualidad/1525080756_303386.html

Hatch, Hans (2020) "Ley Coppa Youtube ¿Qué es?". *Soy.marketing.*
https://soy.marketing/ley-coppa-youtube-que-es

Krivokapic, Djordje; **Adamovic, Jelena** (2016). "Impact of general data protection regulation on children's rights in digital environment". *Anali Pravnog fakulteta u Beogradu*, n. 64, pp. 205-220.
https://doi.org/10.5937/AnaliPFB1603205K

Levanta la cabeza (2019). "Marcas responsables y el nuevo internet de niños". *Levanta la Cabeza*, 12 diciembre.
https://www.levantalacabeza.es/marcas-responsables-y-el-nuevo-internet-de-los-ninos

PwC (2019). *Kids digital media report 2019*.
https://bit.ly/3ewnh7F

Reyes, Irwin; **Wijesekera, Primal**; **Reardon, Joel**; **On, Amit-Elazari-Bar**; **Razaghpanah, Abbas**; **Vallina-Rodríguez, Narseo**; **Egelman, Serge** (2018). "Won't somebody think of the children?" Examining Coppa compliance at scale". *Proceedings on privacy enhancing technologies*, n. 3, pp. 63–83.
https://doi.org/10.1515/popets-2018-0021

Rubio, Isabel (2018). "Estos son los datos que las aplicaciones infantiles más populares recopilan de tus hijos". *Xataca*, 5 octubre.
https://www.xataka.com/privacidad/estos-datos-que-aplicaciones-infantiles-populares-recopilan-tus-hijos

Unión Europea (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).*
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

Valentino-Devries, Jennifer; **Singer, Natasha**; **Krolik, Aaron Keller, Michael, H.** (2018). "How game apps that captivate kids have been collecting their data". *The New York Times*, 12 septiembre.
https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html?curator=-MediaREDE

Yuste, Elisa (2016). "Servicio para el desarrollo de contenido legal para niños". *ElisaYuste*, 3 mayo.
https://www.elisayuste.com/kids-web-services-contenido-legal-para-ninos