Protección del menor en Internet

–

Evita el contenido inapropiado preservando su privacidad

Febrero de 2020

RESUMEN EJECUTIVO

El acceso a contenidos digitales se ha convertido en una realidad en la que no hay ningún colectivo de individuos que no esté de alguna manera expuesto. Cerca del 85% de la población española tiene acceso a internet desde el hogar y, en particular, casi el 70% de menores de 15 años dispone de un teléfono móvil[1].

A pesar de los beneficios que aporta la conectividad actual, existe una serie de riesgos que no debemos olvidar, especialmente en los colectivos más vulnerables como es el caso de los menores, y recordemos que cualquier suceso en la infancia puede tener importantes repercusiones en su desarrollo como adultos. Por lo tanto, si bien el acceso a Internet debe ser tomado como una gran oportunidad para el desarrollo de los menores, los padres o tutores deben tomar medidas para protegerlos de las amenazas del entorno digital al igual que se hace en el mundo físico, y la industria ha de proporcionar herramientas para ayudar a salvaguardar su intimidad y bienestar.

En este documento se presentarán las principales opciones al alcance de padres y tutores para evitar el acceso de los menores a contenido inapropiado. A su vez, se exponen recomendaciones para los desarrolladores de herramientas de protección del menor para que se apliquen las medidas técnicas y organizativas necesarias para proteger los derechos y libertades de los menores.

Palabras clave: menor, control, parental, privacidad, análisis, internet, dispositivo, móvil, RGPD, LOPDGDD, unidad tecnológica, contenido, inapropiado.

[1] INE – España en cifras 2018

ÍNDICE

I. INTRODUCCIÓN

El acceso de menores a contenido inapropiado es una preocupación frecuente para los padres en un mundo cada vez más conectado y con la utilización de dispositivos inteligentes desde edades muy tempranas. Por ejemplo, la edad del primer acceso a contenidos pornográficos en España ha bajado hasta los 8 años, mientras que a partir de los 14 el consumo de este tipo de contenidos es generalizado[2].

Ejemplos de contenido inapropiado para el desarrollo del menor son las imágenes o vídeos con contenido sexual, contenido violento, lenguaje inapropiado, modas que promueven valores negativos que pueden producir riesgos para la salud o malos hábitos, o informaciones falsas o carentes de rigor. El acceso a este tipo de contenido no siempre se produce tras una búsqueda expresa del menor, sino que en muchas ocasiones se produce una exposición "accidental" al aparecer este tipo de contenido de forma inesperada cuando el menor está realizando cualquier actividad en internet.

Las consecuencias para los menores son tan diversas como indeseables, y van desde daños psicológicos y emocionales hasta el establecimiento de conductas peligrosas y socialmente inapropiadas o daños para su salud física.

Existen diversas opciones para evitar que los menores accedan, de forma inadvertida o voluntariamente, a contenido inapropiado cuando utilizan estos dispositivos para navegar, aplicaciones, videojuegos o TV online. Estas opciones, que muchas veces vienen en forma de aplicaciones para dispositivos móviles, pueden llegar a ser muy intrusivas en la privacidad del menor, por lo que es conveniente conocer los riesgos para poder limitarlos[3].

En este documento se presentarán las principales opciones al alcance de padres y tutores para evitar el acceso de los menores a contenido inapropiado, se identificarán los principales riesgos que pueden generarse con su uso y se indican recomendaciones para seleccionar la herramienta apropiada minimizando los riesgos para la privacidad del menor.

A su vez, se exponen recomendaciones para que los desarrolladores de dichas herramientas de protección del menor apliquen las medidas técnicas y organizativas necesarias para proteger los derechos y libertades de los menores.

II. OBJETIVO Y DESTINATARIOS

El objetivo de esta nota técnica es poner de manifiesto el daño que puede producirse a un menor cuando accede a contenido no adecuado para su edad, las opciones que hay al alcance de padres para poder evitar la exposición de sus hijos a este tipo de contenido, las implicaciones para la privacidad de estas herramientas, consejos para un uso responsable de las mismas y recomendaciones para que los desarrolladores de estas cumplan con el RGPD.

Esta nota técnica está dirigida principalmente a padres y tutores de niños que desean fomentar un uso seguro de la tecnología, y para ello necesitan establecer mecanismos que limiten el acceso a contenido inadecuado y permitan controlar el uso de los dispositivos por parte de los niños.

También está dirigido a entidades y desarrolladores que ponen al servicio de padres y tutores estas herramientas a través de las principales plataformas de dispositivos móviles.

[2] Brage, Lluís & Orte, Carmen & Gordaliza, Rosario. (2019). Nueva pornografía y cambios en las relaciones interpersonales de adolescentes y jóvenes.

[3] Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. (2019). Angel or Devil? A Privacy Study of Mobile Parental Control Apps

Por último, esta nota técnica es de interés de editores y publicadores de contenido para adultos.

III. IMPACTO DEL CONTENIDO INAPROPIADO EN LOS MENORES

Antes de abordar cómo puede afectar el acceso a contenido inapropiado es necesario exponer, aunque sea brevemente, las vías por las que los menores pueden acceder a contenido para adultos.

Básicamente el acceso se produce mediante búsqueda/acceso directo o intencionado, acceso indirecto o no intencionado, contenidos de ocio y videojuegos, acceso mediante redes sociales y mediante servicios de publicidad online.

La búsqueda/acceso directo o intencionado se produce cuando los menores acceden a información disponible en internet para saciar su curiosidad, realizando búsquedas sobre temáticas destinadas a adultos en motores de búsqueda y accediendo a contenido que no resulta apropiado para su edad, pero que está fácilmente disponible en internet.

El acceso indirecto se produce cuando el menor encuentra información con contenido inapropiado de forma no intencionada, mientras busca y consulta otro tipo de información.

Contenidos de ocio como cine, televisión, música y videojuegos pueden albergar gran cantidad de contenidos inapropiados para los menores, y a menudo se trata de contenido explícito: violencia, sexo, conductas y valores extremistas, etc.

Igualmente, en redes sociales, incluyendo servicios de mensajería instantánea, correo electrónico, etc., … abundan los fraudes, escondidos detrás de promociones, cupones de descuento y comercio online, así como el intercambio de contenidos inapropiados entre menores (imágenes, vídeos, etc.).

Por último, cabe destacar que en el mundo online la publicidad está siempre presente en forma de ventanas emergentes, banners, videos, etc. y en ocasiones pueden producir la exposición de menores a contenido inapropiado como pornografía, servicios de apuestas, juego, etc.

El acceso a contenido inapropiado puede producir múltiples consecuencias en los menores, tantas como variedades de contenido inapropiado se puedan considerar. El Instituto Nacional de Ciberseguridad (INCIBE) destaca en el marco de su iniciativa Internet Segura para Niños (is4k.es) los siguientes daños potenciales para los menores:

- Daños psicológicos y emocionales. El menor posee una madurez y una autoestima en desarrollo, por lo que es más vulnerable a nivel emocional si tropieza con información que no es capaz de asumir o frente a la que no sabe cómo reaccionar, como por ejemplo contenido pornográfico o violento. Estos les pueden resultar demasiado complejos e incluso perturbadores.
- Desinformación, manipulación y construcción de falsas creencias. Los contenidos falsos y sin rigor pueden confundir a los menores y son especialmente peligrosos cuando tratan temáticas relacionadas con la salud y la seguridad.
- Establecimiento de conductas peligrosas o socialmente inapropiadas. Los menores pueden asumir determinados contenidos como ciertos y positivos, y adoptarlos en forma de conductas o valores dañinos: sexismo, machismo, homofobia, racismo, etc.
- Daños para la salud física. Algunos contenidos tienen como objetivo la promoción de desórdenes alimenticios (anorexia y bulimia), conductas de autolesión o

consumo de drogas. Otros pueden animar a los menores a realizar actividades potencialmente peligrosas para su salud, como algunos vídeos o cadenas virales.

- Inclusión en grupos y colectivos dañinos. Acceder a determinados contenidos puede acercar al menor a colectivos extremistas, violentos o racistas, así como a sectas de carácter ideológico o religioso, grupos políticos radicales, etc. El factor emocional es importante a la hora de hacer frente a esta información que puede ser perjudicial o malintencionada, dado que una baja autoestima, o aquella que esté aún en desarrollo, aumenta la vulnerabilidad del menor.
- Adicciones. El acceso a contenidos inapropiados sobre drogas, sexo y juegos de azar puede favorecer trastornos de adicción, dado que los menores pueden no tener suficiente capacidad crítica para gestionar los riesgos asociados a este tipo de actividades.
- Gastos económicos. Los fraudes o intentos de engaño destinados a estafar a los usuarios para hacerse con su dinero o sus datos pueden acarrear pérdidas económicas directas, como ocurre por ejemplo con las suscripciones de SMS Premium. Además, los menores son más vulnerables a la hora de interpretar y gestionar la publicidad excesiva a la que están expuestos en Internet ya que puede generar en ellos la necesidad de consumir impulsivamente, como sucede con las compras en juegos y aplicaciones. Asimismo, no siempre el contenido de los anuncios es, en sí mismo, adecuado para ellos.

IV. OPCIONES PARA EVITAR EL ACCESO A CONTENIDO INAPROPIADO

A continuación, se expone de forma no exhaustiva una serie de opciones que pueden ayudar a impedir el acceso de los menores a contenido inapropiado, o al menos limitar en la medida de lo posible dicha exposición.

A. BUSCADORES SEGUROS Y APPS DE CONTENIDO EXCLUSIVO PARA NIÑOS

La opción más inmediata y obvia para evitar el acceso de los menores a contenido inapropiado para su edad y nivel de madurez son los buscadores seguros y aplicaciones con contenido exclusivamente dirigido a niños.

Se trata generalmente de buscadores basados en Google SafeSearch que excluyen resultados de búsqueda en base a determinadas palabras filtrada como Kiddle, aplicaciones como YouTube for Kids que restringen la búsqueda de vídeos o aplicaciones con contenido exclusivo para niños como App Movistar Junior, Vodafone Kids Planet y otras. Algunas pueden además limitar el tiempo de uso del navegador o bloquear la pantalla. Son, en general, aplicaciones poco intrusivas en la privacidad del menor, y dada su reducida funcionalidad no requieren de un número elevado de permisos para funcionar. Por el contrario, únicamente son efectivas para menores que utilicen el dispositivo bajo la supervisión directa de un adulto porque simplemente cambiando de aplicación se evitan todas las restricciones.

Algunos dispositivos (Samsung Kids Home) permiten configurar un entorno de aplicaciones permitidas protegido por PIN, de forma que el menor únicamente puede utilizar esas aplicaciones. De esta forma, se pueden ir autorizando accesos a contenido multimedia y nuevas aplicaciones a medida que aumentan las necesidades del menor. Esto se consigue mediante lo que se conoce como un launcher o lanzador. Un launcher es el equivalente a un escritorio en Android, muestra los iconos de algunas aplicaciones y permite ejecutarlas, así como la imagen del fondo de pantalla, pero manteniendo ocultos los iconos de las aplicaciones prohibidas, que no pueden ser ejecutadas. Esta modalidad permite más

autonomía del menor con el dispositivo, ya que podrá cambiar entre las aplicaciones y contenidos autorizados, pero son efectivas únicamente entre los más pequeños por la estética y grandes restricciones que imponen.

B. CONTROL PARENTAL OFRECIDO POR LOS SISTEMAS OPERATIVOS DE LOS FABRICANTES

Los grandes fabricantes de sistemas operativos para dispositivos móviles ofrecen soluciones muy completas, bien integradas en el sistema y gratuitas o incluidos en la licencia del propio sistema operativo. Es el caso de Family Link de Google para dispositivos Android, o Control Parental Apple para dispositivos iOS. En el primer caso se instala como una aplicación independiente y gratuita desde Google Play Store, en el segundo de los casos viene integrado en el propio SO y únicamente hay que activarlo y configurarlo.

En el caso de Microsoft, también existe la posibilidad de establecer configuraciones de control parental en Windows 10, con algunas funcionalidades disponibles en Android a través de la aplicación Microsoft Launcher, también viene integrado en propio sistema operativo, pero que no incluye el filtrado de contenido web.

Tanto en el caso de Google como en el caso de Microsoft es necesario crear una cuenta de usuario específica para los menores, indicando su edad, y que serán autorizadas y gestionadas desde una cuenta de usuario de un adulto.

A pesar de estar bien integradas en el sistema, no están exentas de limitaciones. Por ejemplo, con Family Link el filtrado de contenido únicamente funciona cuando se utiliza Chrome para navegar, siendo necesario bloquear la instalación y uso de otros navegadores. En el caso de Microsoft el bloqueo de contenido únicamente funciona en dispositivos con Windows 10 y navegador Edge, siendo necesario bloquear la instalación y uso de otros navegadores.

Además del filtrado de contenido, en líneas generales las tres opciones ofrecen funcionalidades parecidas como el control/bloqueo de aplicaciones, control de tiempo de uso y localización GPS.

La amplia gama de funcionalidad que ofrecen hace que estas aplicaciones tengan que acceder a un número elevado de recursos protegidos del sistema y realizar tratamientos de datos personales de gran volumen y complejidad en relación con el menor, por lo que pueden resultar muy intrusivas para la privacidad del menor.

Aun así, en los casos en los que están integrados en el sistema operativos no requerirán apenas permisos al usuario ya que pueden acceder a los recursos a través de los privilegios del propio sistema operativo.

Es por eso mismo, que resulta vital que tales aplicaciones realicen un ejercicio de transparencia esencial en sus políticas de privacidad y ofrezcan suficiente granularidad sobre los tratamientos a realizar.

C. OTRAS APLICACIONES DE CONTROL PARENTAL

Existe una amplia gama de aplicaciones de control parental en el mercado que permiten bloquear el acceso de menores a contenido inapropiado. Una buena recopilación de estas herramientas, además de una guía de selección, está publicada en la web de is4k de INCIBE. Tienen funcionalidades muy diversas, como control de tiempo, filtrado de contenidos, bloqueo de aplicaciones, seguimiento de actividad, alertas y notificaciones, control multidispositivo, geolocalización, etc. Sin embargo, no todas impiden el acceso a contenido inapropiado, por lo que es importante seleccionar una que incluya filtrado de contenido y bloqueo de aplicaciones.

Al igual que en los casos anteriores, se trata de aplicaciones que, por sus características, pueden acceder a información sensible del tráfico, la actividad del menor en internet e incluso su localización física, por lo que es recomendable seleccionar la aplicación cuidadosamente en función de la granularidad que ofrezca en las funcionalidades que proporciona y prestar atención a la política de privacidad de cada una de ellas antes de instalarlas.

Aquellas que entre sus funcionalidades permiten el control de la actividad del menor en redes sociales necesitarán además tener acceso a las cuentas de usuario de las redes sociales, y acceso por tanto a toda la información del menor en esas redes sociales. A la vez que proporcionan una capacidad de control extraordinaria, que puede ser apropiada en determinadas circunstancias, pueden suponer una intrusión excesiva en la privacidad del menor. Todas las aplicaciones de redes sociales incluyen controles de privacidad para controlar/limitar la interacción del menor con desconocidos, censurar los mensajes que se reciben en base a su origen y contenido, etc. En la web de is4k se incluyen orientaciones para sacar el máximo provecho es estas opciones de privacidad.

Estas aplicaciones requerirán del usuario un número elevado de permisos para acceder a recursos del sistema, que una vez concedidos dotan a las aplicaciones de acceso a una variedad y volumen de información tradicionalmente reservada al sistema operativo[4].

Por tanto, a estas aplicaciones también debe exigírseles una transparencia ejemplar de cara a los tratamientos de datos personales que realizan y una aplicación de medidas de seguridad técnicas y organizativas del más alto nivel de cara a minimizar los riesgos para los derechos y libertades de los menores.

Algunas de las más conocidas Qustodio, Norton Family, Kaspersky Safekids, F-Secure Mobile Security y Securekids.

D. OPCIONES DE CONTROL PARENTAL OFRECIDO POR LOS OPERADORES DE TELEFONÍA

Los operadores tradicionales de telefonía en España disponen de la opción de contratar un servicio de control parental (Movistar Protege, Vodafone SecureNet y Orange Kids Ready) con un coste adicional y que requiere la instalación de una app específica en cada dispositivo a controlar. Permiten gestionar la actividad de los niños en internet, filtros de contenido (adultos, violencia, redes sociales, …), definir periodos de conexión, bloqueo de aplicaciones y otras funcionalidades desde un único punto que controla los dispositivos gestionados. En el caso de Movistar, está basado en otra aplicación comercial de control parental llamada Qustodio.

Únicamente Orange dispone de una tarifa específica para menores llamada Orange Kids que incluye de forma gratuita y por defecto la protección del servicio Orange Kids Ready.

E. ALTERNATIVAS AL USO DE APLICACIONES DE CONTROL PARENTAL

Existen algunas alternativas para evitar la instalación de aplicaciones de control parental pero que requieren cierto conocimiento técnico. Una de ellas es la opción de filtrado DNS de contenido ofrecida por OpenDNS (Family Shield), CleanBrowsing y otros. Esta se configura en el router[5] de casa, cambiando los servidores DNS que configura el suministrador de internet por otros servidores DNS que filtrarán las peticiones de acceso a webs de contenido inapropiado (adultos, juegos, apuestas, torrents, redes sociales, etc) en base a filtros configurables. Puede ser muy efectivo para todos los dispositivos conectados a la red de casa (WiFi o cable), como móviles, tablets, ordenadores, videoconsolas y smartTVs, pero

[4] Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. (2019). Angel or Devil? A Privacy Study of Mobile Parental Control Apps

[5] Ejemplos de configuración de routers domésticos para utilizar OpenDNS o CleanBrowsing

difícil de gestionar para conexiones de datos móviles y en otras redes WiFi. En el pasado los operadores de telefonía ofrecían servicios de este tipo de forma sencilla para sus clientes de ADSL, como CanguroNet de Telefónica.

Estas alternativas se pueden utilizar en combinación con algunos de las aplicaciones de control parental expuestas con anterioridad.

F. CONTROL PARENTAL EN OTROS DISPOSITIVOS

Control parental en servicios de TV y Vídeo en streaming

Las grandes plataformas de TV y vídeo en streaming (HBO, Netflix, VodafoneTV, Movistar+, OrangeTV) ofrecen la opción de bloquear el acceso a determinados contenidos mediante el establecimiento de un código de acceso.

Control parental en dispositivos de juego

Todas las consolas de videojuegos disponen de algún sistema de control parental, lo que permite a los padres proteger la seguridad de sus hijos y mantener un nivel de privacidad adecuada. Estas aplicaciones permiten entre otras cosas seleccionar a qué juegos pueden jugar los niños según la clasificación PEGI, limitar y supervisar las compras online, limitar el acceso a navegación por internet desde el dispositivo, poner límites al tiempo de juego y controlar el nivel de interacción online en chats de juego.

G. MÉTODOS DE CONTROL POR PARTE DE EDITORES Y PUBLICADORES DE CONTENIDO

Hasta el momento, no hay constancia de que editores y publicadores de contenido para adultos en España utilicen algún método efectivo para verificar la mayoría de edad de los usuarios, más allá de peticiones al propio usuario para confirmar su mayoría de edad.

Sin embargo, existen en el mercado soluciones que podrían dar respuesta a esta problemática como AgeID, AgeChecked, AgePass, y Yoti entre otras. Se trata de servicios de terceros que se encargan de verificar la identidad y/o edad del usuario mediante un documento como el pasaporte o carnet de conducir. Una vez verificada la mayoría de edad la información personal es cifrada o destruida, de forma que únicamente se conserva y comparte con el servicio de contenido para adultos si el usuario es mayor de edad o no.

En el caso de Yoti, ofrece la opción de verificar la mayoría de edad sin necesidad de aportar ningún documento, se realiza mediante tecnologías de análisis facial. Para evitar falsos positivos el sistema estimará si el usuario es mayor de 25 años o no, y ese es el único dato que se comparte con el servicio online de contenido para adultos. Este servicio se puede probar en https://www.provemyage.com/. Yoti es además la única solución certificada por el regulador británico (British Board of Firm Classification), en base a un esquema de certificación para sistemas de verificación de edad que incluye, entre otros, requisitos de protección de datos.

La evolución hacia herramientas de este tipo supondría un gran avance en términos de responsabilidad proactiva por parte de los responsables de tratamiento.

V. PRINCIPALES MÉTODOS PARA ELUDIR EL CONTROL PARENTAL

Los métodos de control presentados en esta nota técnica no son infalibles y si el menor tiene cierto interés y curiosidad puede llegar a encontrar mecanismos para saltarse los límites de acceso a contenido. Incluso careciendo de dicho interés, y a pesar de las medidas

los menores podrán seguir accediendo a contenido de este tipo de forma colateral. Los principales mecanismos para evitar el control de acceso a contenido son:

1. Uso de proxy online para acceder a contenido web restringido. Por ejemplo, desde https://www.hidemyass.com/es-es/proxy se puede navegar a otras páginas restringidas. Estas páginas que funcionan a modo de proxy pueden bloquearse específicamente, pero es necesario estar atento y bloquearlas si se detecta su uso.
2. Descubrimiento de contraseña. A menudo los menores son capaces de descubrir la contraseña/PIN de acceso a la gestión del control parental.
3. VPNs. La conexión a través de VPNs (gratuitas o de pago) puede producir un efecto similar al uso de proxies, perdiendo todo el control posible sobre el filtrado de contenidos.
4. Conexión a redes (WiFi) no protegidas, por ejemplo, la WiFi de centros comerciales o restaurantes. Si se opta por soluciones de filtrado de contenido basadas en filtrado de peticiones DNS de la red de casa, mediante la conexión a otras redes WiFi el menor podrá navegar sin ningún tipo de filtro. Las aplicaciones de control parental suelen ser capaces de filtrar independientemente de la red de acceso a internet que se utilice.
5. Navegadores portables. Algunas herramientas de control parental únicamente filtran contenido en determinados navegadores web. Es necesario bloquear la instalación de otros navegadores para impedir el acceso a contenido inapropiado. Pero algunas plataformas permiten la utilización de navegadores portables que no requieren instalación y pueden ser utilizados para evitar el filtrado de contenidos.
6. Visionado de contenido a través de servicios no bloqueados como Google Images, Google Translate, Wikipedia, Whatsapp, Telegram, …

Una vez expuestos estos mecanismos, queda patente que las distintas opciones de control parental no son infalibles y la única forma de atajar esta suerte de vulnerabilidades es complementar el uso de estas herramientas con una educación adecuada sobre el uso seguro de la tecnología, los peligros de internet y la importancia de que ellos mismos sean capaces de tomar sus propias medidas.

Además, es interesante y necesario configurar adecuadamente las opciones de privacidad y seguridad de aquellas aplicaciones que lo permitan. Hacer un buen uso de estas funciones es fundamental para conseguir un control parental más eficaz. En la iniciativa IS4K de INCIBE se pueden encontrar orientaciones para configurar aplicaciones como Instagram, TikTok, YouTube, Whatsapp, etc.

VI. RECOMENDACIONES PARA PADRES Y TUTORES

En función de todo lo expuesto anteriormente, se establecen una serie de recomendaciones para padres y tutores:

1. Educa a los menores sobre los riesgos para su privacidad y su seguridad en el uso de tecnologías móviles. Fomenta el uso responsable de la tecnología.
2. Limita a los menores el tiempo de uso de los dispositivos conectados.
3. Hazles saber que es necesario tomar medidas por su propia seguridad. Cuéntales que tomas esas medidas por su propio bien.
4. Emplea sistemas operativos, proveedores de internet y terceros que faciliten opciones de control parental que permitan monitorizar el uso de dispositivos móviles.
5. Configura las opciones de control parental, ya que ofrecen diferentes funcionalidades como el filtrado de contenido, limitación de horarios, bloqueo de aplicaciones, detalles de uso de las redes sociales, localización GPS, etc.

6. Elige la herramienta que mejor se ajuste a tus necesidades y ofrezca garantías para no introducir nuevos riesgos.
7. Infórmate de los periodos de retención de datos y asegúrate de que no se utilizan los datos para finalidades distintas de las que necesitas[6].
8. Emplea navegadores, launchers y aplicaciones en su versión infantil que son alternativas que pueden ser menos intrusivas.
9. No olvides que otros dispositivos conectados como SmartTV o videoconsola están expuestos a riesgos similares.
10. Ten en cuenta que algunas herramientas bloquean en exceso, mantenga abierta la posibilidad de desbloquear contenido a petición del menor y esté abierto a acordar con ellos los filtros y restricciones a configurar. Un bloqueo excesivo puede ser contraproducente.
11. Recuerda que las herramientas de control parental no son infalibles, así que configura adecuadamente las opciones de privacidad y seguridad en aplicaciones y redes sociales[7], manténgase alerta y en comunicación con sus hijos.

VII. RECOMENDACIONES PARA LA INDUSTRIA

Dado que este tipo de servicios de control parental se ofrecen principalmente a través de aplicaciones en dispositivos móviles, es necesario que la industria, proveedores de servicio y desarrolladores, tengan en consideración las recomendaciones establecidas en la nota técnica sobre el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos[8] móviles publicada por esta Agencia.

Además, dada la naturaleza intrusiva de este tipo de aplicaciones, motivada por la gran cantidad de funcionalidad que ofrecen y las características especiales del público al que van dirigidas, se deben aplicar medidas técnicas y organizativas en función del nivel de riesgo para los derechos y libertades de los menores.

Además de las directrices recogidas en la nota técnica anterior, sin ánimo de exhaustividad, los prestadores de servicio de aplicaciones de control parental deben considerar las siguientes recomendaciones:

1. Aplicación del principio de minimización de datos. Si bien estas aplicaciones suelen ofrecer funcionalidades muy diversas, no siempre será necesario que los padres utilicen todas ellas. Debe ofrecerse granularidad en este sentido, estableciendo mecanismos que permitan activar y desactivar cada una de esas funcionalidades en base a las necesidades de cada familia. Los datos personales que correspondan a una funcionalidad desactivada no deberán ser tratados.
2. Minimización de permisos. De forma análoga al punto anterior, deben establecerse mecanismos para no solicitar permisos de acceso a recursos del sistema innecesarios para las funcionalidades que se van a utilizar. A modo de ejemplo, si un usuario no necesita utilizar la funcionalidad de localización GPS del menor, no parece necesario que la aplicación tenga que acceder a datos de geolocalización de forma continua e incluso en segundo plano.
3. Gestión de librerías de terceros. Prácticamente todas las aplicaciones incluyen librerías de terceros para añadir funcionalidad muy diversa como estadísticas de uso, informes de error, autenticación de usuarios o publicidad. En tal caso, debe informarse a los interesados de los tratamientos de datos personales que puedan introducir tales librerías de forma que se pueda obtener un consentimiento válido antes de que dichos tratamientos se lleven a cabo. Debe evitarse realizar cesiones

[6] AEPD - Decálogo para la adaptación al RGPD de las políticas de privacidad en internet.
[7] is4k -Configuraciones de seguridad, privacidad y control parental en las aplicaciones de moda.
[8] AEPD – Nota Técnica: El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles.

de datos personales, incluidas transferencias internacionales de datos, para las que no se tenga una base legitimadora y sin que se haya informado adecuadamente.

4. Establecer garantías en los servicios en la nube. Estrechamente relacionado con el apartado anterior, todas las aplicaciones móviles requieren un conjunto similar de características ofrecidas a través de backends. En algunos casos se utilizarán backends ofrecidos por terceros para cada una de funcionalidades, en otros casos esos backends serán desarrollados a medida para la aplicación concreta y consumidos desde la app mediante una API. Independientemente de la modalidad, lo habitual es que esos backends estén alojados en servidores en la nube. En tal caso, los tratamientos que realicen estos proveedores de servicios en la nube deberán estar regulados por un contrato o vínculo legal que cumpla los requisitos establecidos en el RGPD. El responsable de tratamiento deberá mostrar diligencia en la selección de los proveedores de servicios en la nube y en el contrato de encargo de tratamiento deberá cumplir los requisitos establecidos en el RGPD, poniendo especial atención a las medidas de privacidad desde el diseño, por defecto, de seguridad, compromiso de confidencialidad y procedimiento de gestión de brechas de seguridad. Para más información pueden consultarse la guía sobre contratación de servicios en la nube[9] publicadas por la Agencia. Si bien la contratación de este tipo de servicios suele realizarse mediante la adhesión a cláusulas contractuales establecidas por el prestador de servicios en la nube, éstos deberán o bien adaptar dichas clausulas a los requisitos del RGPD o bien dotar de flexibilidad suficiente a los sistemas de contratación para que los contratos establecidos puedan dar cumplimiento a las exigencias del RGPD.
5. Aplicar medidas de seguridad. Teniendo en cuanta el volumen, categorías y el perfil de los individuos sobre los que se realiza el tratamiento se deben maximizar las medidas aplicando los más altos estándares de seguridad.

VIII. CONCLUSIONES

El uso de tecnologías móviles conectadas por parte de menores de edad se extiende cada vez más y resulta una tendencia imparable por las innumerables ventajas que presenta para su desarrollo y formación. Sin embargo, también presenta algunos riesgos que es necesario resolver.

Uno de los riesgos más importantes es la exposición de los menores a contenido inapropiado como imágenes de índole sexual, violentas, sobre juego y apuestas, etc. Esta exposición puede producir importantes efectos negativos sobre los menores, que van desde daños emocionales o psicológicos hasta el establecimiento de conductas peligrosas y socialmente inapropiadas o daños para su salud física.

En esta nota técnica se han ofrecido diversas opciones, a disposición de padres y tutores, para controlar y limitar la exposición de los menores a contenido inapropiado.

La primera de ellas es el uso de buscadores, aplicaciones dirigidas específicamente a niños y launchers que impiden que el menor acceda a otro tipo de aplicaciones. Se trata de una opción relativamente sencilla y efectiva a edades tempranas, pero requieren una vigilancia.

En segundo lugar, están las aplicaciones de control parental que ofrecen los propios desarrolladores de sistemas operativos, operadores de telefonía y otras empresas. Se trata de opciones que, además del filtrado de contenidos, ofrecen funcionalidades adicionales

[9] AEPD – Guía para clientes que contraten servicios de Cloud Computing y Orientaciones para prestadores de servicios de Cloud Computing.

como control de tiempo de uso de dispositivos, bloqueo de acceso a aplicaciones, control de tiempo de uso por aplicación, control de actividad en redes sociales, gestión remota para padres y tutores e incluso localización GPS del menor en tiempo real.

Para poder ofrecer todas estas funcionalidades estas aplicaciones requieren numerosos permisos de acceso a recursos protegidos del dispositivo y tratar un volumen muy elevado de datos personales del menor. En definitiva, son opciones que, aunque sean efectivas en cuanto a la finalidad de control que persiguen, también son muy invasivas para la privacidad el menor.

Antes de seleccionar una aplicación de control parental es importante obtener información precisa sobre los tratamientos de datos personales que llevará acabo la aplicación, especialmente medidas de seguridad, tiempos de retención de datos, posibles cesiones de datos, una clara identificación del responsable de tratamiento y cómo ejercer los derechos que confiere el RGPD. También es importante seleccionar aquella opción que mejor se ajuste a la funcionalidad que se necesite, teniendo en cuenta que, a mayor funcionalidad, mayor invasión potencial en la privacidad del menor y mayor riesgo de que un incidente de seguridad pueda afectar a sus derechos y libertades. Hay que prestar especial atención a la configuración de privacidad de cada una de las aplicaciones o redes sociales que utilice el menor.

Quienes ponen a disposición de padres y tutores este tipo de aplicaciones deben ser ejemplares en el ejercicio de transparencia y responsabilidad activa, ofreciendo granularidad suficiente en las funcionalidades que se ofrecen y por tanto en los tratamientos de datos personales que se realizan. Es decir, aunque una aplicación pueda ofrecer localización precisa del menor, si los padres no consideran necesaria su utilización deben poder prescindir del tratamiento y denegar los permisos de acceso asociados a dicho tratamiento sin que eso impida la utilización de la aplicación.

Como alternativa a las aplicaciones de control parental, existen otras herramientas que permiten evitar el acceso a contenido inapropiado mediante la configuración de servidores DNS que filtrarán y no resolverán aquellas peticiones que puedan dirigir al menor a este tipo de contenido. Son soluciones bastante efectivas en las WiFis domésticas, pero que pierden su efectividad cuando el dispositivo se conecta a otra red o utiliza conectividad de telefonía móvil.

Además de las acciones que son responsabilidad de los padres, se han presentado también algunas opciones para que publicadores y editores puedan evitar el acceso de menores a contenido inapropiado. Por el momento controles de ese tipo no son muy populares, pero es de esperar que poco a poco su implantación sea mayor. Este tipo de medidas pueden considerarse como ejemplos de responsabilidad activa en la aplicación del principio de minimización de datos.

Adicionalmente, se presentan en esta nota técnica algunas de las principales técnicas mediante las cuales el menor podría eludir el control parental, algunas de ellas requieren ciertos conocimientos técnicos, pero muchas otras están prácticamente al alcance de cualquiera con un nivel de curiosidad y motivación suficiente.

Para finalizar y a modo de recopilación de todo lo expuesto durante la nota técnica se ofrece una lista de consejos para poder evitar los daños que puede producir el acceso a contenido inapropiado por parte del menor, pero al mismo tiempo con el máximo respeto a su privacidad e intimidad.

IX. REFERENCIAS

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).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

https://www.is4k.es/necesitas-saber/contenido-inapropiado

https://www.is4k.es/de-utilidad/herramientas

Brage, Lluís & Orte, Carmen & Gordaliza, Rosario. (2019). Nueva pornografía y cambios en las relaciones interpersonales de adolescentes y jóvenes.

Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla(2019). Angel or Devil? A Privacy Study of Mobile Parental Control Apps

AEPD - Decálogo para la adaptación al RGPD de las políticas de privacidad en internet.

AEPD – Nota técnica: El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles.

AEPD – Guía para clientes que contraten servicios de Cloud Computing.

AEPD – Orientaciones para prestadores de servicios de Cloud Computing.

Mobile Security Framework - MobSF

Control Parental iOS – Política de privacidad

Control Familiar Microsoft – Política de privacidad

Family Link – Política de privacidad

Movistar Protege – Política de privacidad

Vodafone Securenet – Política de privacidad

Orange Kids Ready – Política de privacidad

Kaspersky Safekids – Política de privacidad

Securekids – Política de privacidad

Qustodio – Política de privacidad

F-Secure Mobile Security – Política de privacidad

Norton Family – Política de privacidad

X. ANEXOS

Tabla comparativa de las herramientas de control parental analizadas

HERRAMIENTAS CONTROL PARENTAL	CVSS - MobSF	Score - Seguridad MobSF	Nº Permisos solicitados - MobSF	Trackers - MobSF	Filtro contenidos	Control de Tiempo	Bloqueo/Control Apps	Historial de actividad en redes sociales	Control de llamadas / SMS	Seguimiento GPS	Gestión remota / Aplicación Pad	Sistemas Operativos	PRECIO
KASPERSKY SAFEKIDS	6	15/100	27	5	Sí	Sí	Sí	En versión de pago (Facebook)	No	En versión de pago	Sí	PC, Mac y Android (En iOS sólo filtro de contenidos)	Version Gratuita y Versión Premium - 14,95€/año
FAMILY LINK	6,3	0/100	9	1	Sí	Sí	Sí	No	No	Sí	Sí	Android	Gratuito
SECUREKIDS	6,1	10/100	36	5	Sí	Sí	Sí	No	No	Sí	Sí		Gratuita
QUSTODIO	5	65/100	24	7	Sí	Sí	Sí	Sí (Facebook, Youtube)	Sí	Sí	Sí	Windows, Mac, Android, iOS, Kindle	Gratuito 30 días y después 42,95€/año (hasta 5 dispositivos)
CONTROL FAMILIAR MICROSOFT (LAUNCHER)	*	*	*	*	Sí	Sí	Sí	No	*	Sí	Sí	Windows (PC y móvil) En Android (con Microsoft Launcher	Incluido en Windows
CONTROL PARENTAL IOS	*	*	*	*	Sí	*	Sí	No	No	No	No	iOS (iTunes en PC y Mac)	Incluido en iOS
F-SECURE MOBILE SECURITY	6,2	10/100	48	2	Sí	Sí	Sí	No	No	No	No	Android	7,45€ / 6 meses
NORTON FAMILY	5,7	10/100	10	4	Sí	Sí	Sí	Sí	No	No	Sí		
MOVISTAR PROTEGE	5,5	25/100	22	4	Sí	Sí	Sí	Sí (Facebook, Youtube)	Sí	Sí	Sí	Windows, Mac, Android, iOS, Kindle	2,99€/mes (hasta 10 dispositivos)
CIBERALARMA	5	65/100	6	1	Sí	No	No	Sí	No	No	Sí	Android	11,90€/año 1 dispositivo / 56,90€/año 5 dispositivos
VODAFONE SECURENET	6,3	10/100	12	2	Sí	Sí	No	No	No	No*	Sí	Android, iOS	Gratis en algunas tarifas altas y 1€/mes en el resto
ORANGE KIDS READY	5,2	55/100	19	4	Sí	Sí	Sí	No	No	Sí	Sí	Android, iOS	2,95€/mes (hasta 10 dispositivos)
Modo Niños Samsung (Launcher)	6,1	45/100	9	0	Sí	Sí	Sí	No	Sí	No	No	Android	Incluido en móviles Samsung

En esta tabla se incluyen los valores de cuatro parámetros obtenidos mediante el análisis estático de las aplicaciones de control parental que aparecen en la misma. La herramienta utilizada para el análisis es Mobile Security Framework, herramienta de código abierto y libre. Se han analizado exclusivamente las versiones Android de las aplicaciones relacionadas. A continuación, se detalla el significado de cada uno de los parámetros.

Parámetro	Significado
CVSS- MobSF	Sistema de puntuación diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información. Se obtiene una media de las potenciales vulnerabilidades detectadas. La severidad se considera baja si la puntuación obtenida está entre 0.0 y 3.9. LA severidad es media si el resultado se ubica entre 4.0 y 6.9. Se considera alto cuando la puntuación está entre 7.0 y 10.0
Score – MobSF	Puntuación de seguridad obtenido por MobSF en una escala de 0 a 100, en función del análisis estático. Basado en la metodología OWASP
Número de permisos solicitados – MobSF	Número de permisos de acceso a recursos del sistema declarados en el código de la aplicación y que se solicitarían al usuario.
Trackers - MobSF	Número de librerías o urls de trackers detectados en la aplicación.