GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

MONOGRÁFICO GESTIÓN DE LA PRIVACIDAD E IDENTIDAD DIGITAL

MONOGRÁFICO GESTIÓN DE LA PRIVACIDAD E IDENTIDAD DIGITAL

1. Objetivo del monográfico

"Aprender y transmitir la importancia de que los menores gestionen su visibilidad, reputación y privacidad en la red, así como su huella digital en internet".

2. Conceptualización y descripción del riesgo

El desarrollo de las tecnologías de la información y su uso intensivo por parte de los ciudadanos plantea nuevos retos para una adecuada gestión de la privacidad. Si se echa la vista atrás, se puede observar la considerable evolución que se produjo entre la web 1.0 y la web 2.0. Mientras en la web 1.0 tan solo se ponía consumir contenido sin posibilidades de interacción, la lógica de la WEB 2.0 introdujo el concepto de compartir y colaborar entre sí funcionando, por ejemplo, como creadores de contenido tal como se puede comprobar en herramientas como blogs, wikis, servicios de alojamiento de videos o redes sociales. Así, el internauta colabora, comparte e interactúa con los demás usuarios creando una gran comunidad virtual, colaborando en que la información circule rápidamente en la red y por lo tanto, surge el riesgo de que pueda llegar de modo indeseado. Por ello, a pesar de los evidentes avances reportados por la mencionada evolución, no se ha de olvidar el hecho de que crear, compartir y mostrar contenido puede conllevar determinados riesgos para la privacidad y para la generación de la propia identidad digital.

"LA INFORMACIÓN ES PODER"

¿Qué es la "*privacidad*"?

Privacidad: "*Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"[1].

La **privacidad en Internet** se refiere al control de la información personal que posee un usuario que se conecta a la Red, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación.

[1] Real Academia Española. (2001). Privacidad. En Diccionario de la lengua española (22.a ed.). Recuperado de http://lema.rae.es/drae/?val=privacidad

La privacidad debe entenderse como **"**un tesoro**"** que se comparte con los más cercanos y no se deja al alcance de personas desconocidas o ajenas a nuestra confianza. Por ello, llevar a cabo una buena gestión de la privacidad es muy importante para evitar problemas y estafas ya que los datos personales no solo dicen el nombre y el domicilio, sino que además definen a la persona, mostrando aficiones, gustos, tendencias o creencias. Si no se protege esa información, puede ser usada de forma fraudulenta.

Cuando se habla de protección de datos personales se hace referencia tanto a toda aquella información que identifica a la persona o que la puede hacer identificable como a aquella que habla de ella misma. Es decir, gestionar la privacidad no sólo significa gestionar los datos personales de forma exclusiva sino que también debe abarcar aquella información que habla sobre las preferencias, gustos, comentarios, ideas, etc. En este sentido, que un menor comente a través de una red social determinada que odia a los profesores de su colegio o que defiende la discriminación, se configura como una mala gestión de la privacidad de éste. Todo ello influye de forma directa y negativa en la creación de su identidad digital y reputación personal. Por ello, se debe concienciar a los menores de la importancia que tiene **«pensar antes de publicar»** en las posibles consecuencias que pueda tener en su futuro lo que en el presente expone de sí mismo. De este modo, saber gestionar la privacidad en el sentido amplio del que se está hablando resulta fundamental para construir una adecuada identidad digital y reputación que sea de provecho para el futuro del menor.

Son datos personales: el nombre y apellidos, el DNI, una fotografía, la dirección, el número de teléfono, la voz...

Los datos personales lo dicen todo de uno: quién es, dónde vive, qué hace, qué le gusta…

Toda persona tiene derecho a la protección de sus datos de carácter personal, es decir, tiene derecho a decidir sobre quién tiene datos personales suyos y a saber para qué los usan una organización y deben siempre informar de cómo modificarlos o cómo borrarlos de sus ficheros de datos.

La **falta de privacidad en Internet** es una realidad que ya está haciendo cambiar las vidas de todos, creando víctimas y teniendo consecuencias muy graves en personas que, sin saberlo, han hecho de su vida algo público. Así, los términos de ciudadanía y

vida social han cambiado rápidamente en la era digital, observándose una tendencia hacia el uso de formas públicas como modalidad por defecto frente a una disminución del empleo de estrategias de comunicación privadas[2]. Así, para poder "existir" on-line las personas tienden a publicar contenidos públicos que podrán ser compartidos a su vez por otros usuarios, escapando así de la sensación de no formar parte de grupos o comunidades de referencia para los mismos y vulnerando en ciertas ocasiones su propia seguridad.

Estándares de seguridad en la Red

Así, para comprender el gran reto que supone mantener el equilibrio entre seguridad y privacidad con la interacción en la red y utilidad en Internet, resulta interesante hacer referencia a algunos de los principales conceptos para definir la seguridad en la red:

- **Confidencialidad:** implica que la información tan sólo podrá ser accesible a aquellas entidades o personas autorizadas a las que el usuario dé su consentimiento. Así, y especialmente en las redes sociales, este estándar resulta de vital importancia porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.

- **Integridad:** la información que aparece en la red sólo puede ser modificada por las entidades o personas autorizadas.

- **Autenticación:** es necesario establecer mecanismos de verificación de la identidad digital de las personas y entidades en la red para poder controlar que el usuario sea realmente quién dice ser.

Todos estos estándares deben estar presentes como punto de partida para mantener la privacidad y la seguridad en la red. Así, la Ley de Protección de Datos[3] alcanza una importancia exponencial dentro del ámbito de las nuevas tecnologías, asegurando que no se produzca divulgación ilícita ni uso indebido de información privada de los usuarios.

De este modo, abordar la privacidad en el contexto de Internet implica atender a varios puntos:

[2] Pew Research Center (2014). *The Future of Privacy*. Recuperado de http://www.pewresearch.org/
[3] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE nº 298 de 14 de diciembre de 1999.

- **Privacidad y anonimato de la identidad digital**: existen espacios donde poder actuar bajo un "nick"[4] y otros donde se requieren de una identificación real del usuario. Es importante valorar, teniendo en cuenta el entorno donde se encuentre la persona, qué forma de identificación se va a usar: anónima o personal, ya que esto influirá en la identidad digital y en la interacción con el resto de usuarios de la red.

- **Privacidad de nuestros datos personales:** en muchos portales e incluso en las redes sociales existe la posibilidad de realizar un registro privado, aunque también es probable que se ofrezca la oportunidad de que los datos aportados puedan ser públicos, atendiendo a qué usuarios podrán tener acceso a los mismos. Así, antes de facilitar los datos o dejar abierto nuestro perfil, se debería valorar quién va a tener acceso a ellos y cuál podría ser el uso que se hiciera de los mismos.

Por lo tanto, y a modo de resumen, se puede decir que, al igual que se activan pautas de seguridad y privacidad en nuestra vida real, la privacidad ha de estar presente cada vez que se interacciona en la red. Por ello, resulta imprescindible que se sea capaz de interiorizar esta necesidad y se aprenda a aplicar sus bases en el propio entorno digital. Así, como padres, madres, tutores o educadores, se debe saber transmitir a los menores la importancia de la privacidad y que tienen que tener cuidado con quién comparten información en la Red pues se está a tiempo de tomar medidas que garanticen que a las zonas de privacidad sólo entren las personas a quienes se ha invitado a entrar.

Motivaciones de los menores para su exposición en Internet

Una de las razones a destacar por la que los menores se exponen tanto en Internet es el efecto de notoriedad o popularidad que puede producir la participación en los entornos digitales. Así, en el caso de las redes sociales, la popularidad puede medirse tanto por el número de "amigos" registrados en nuestro perfil como por la cantidad y calidad de interacciones que se produzcan sobre la actividad en la red. De este modo, y especialmente en la infancia y adolescencia, sentir el reconocimiento social y la aceptación del otro sobre la propia persona es un aspecto clave en el desarrollo del

[4] Palabra, nombre, sobrenombre, alias o pseudónimo que utiliza un usuario en los medios digitales para identificarse y poder comunicarse.

autoconcepto y la autoestima, especialmente en el entorno cercano entre iguales, ya que son a quieres consideran importantes para su definición y encaje social o pertenencia a un grupo.

Además de la evidente influencia que pueden tener sobre los menores los iconos populares de referencia para los mismos en esta exposición (ídolos cuya forma de vida y comportamiento se configuran como ejemplos a seguir también en la búsqueda de notoriedad y seguidores) no se debe olvidar que, por medio de la comparación social, los menores pueden llegar a incrementar su exposición en la red para demostrar su propia existencia, para enseñar su vida, y en definitiva, autoafirmarse en sí mismos. Igualmente, dentro del sector juvenil este comportamiento es más común ya que en muchos casos no son conscientes de las consecuencias que, incluso a nivel legal, esta exposición puede llegar a tener.

Por último, se ha de tener en cuenta que en la adolescencia los jóvenes buscan experiencias nuevas, tener un público que siga sus incursiones o con quién sentirse identificados, objetivo amplificado gracias a la sensación de anonimato que ofrece la red.

¿Qué es la identidad digital?

Actualmente los límites entre la identidad analógica y digital, es decir, entre quien soy y quién soy en Internet, son cada vez más difusos. Resulta interesante por lo tanto hablar de una identidad cada día más unitaria y global que se desarrolla y actúa constantemente y de forma paralela en la vida cotidiana de cada persona, adultos en general y menores en particular.

Así, la identidad es el resultado de la vida diaria, de lo que se hace y se publica en redes sociales personales y profesionales, de los comentarios en foros y blogs, de las imágenes subidas a Internet, de los videos publicados en Youtube o de la opinión de nuestros contactos y seguidores. Se habla por lo tanto de una identidad que se conforma por lo que se sube a Internet de cada persona, tanto por ella misma como por amigos, compañeros, familiares, etc., por lo que esa identidad a veces puede dar una imagen no muy real de su persona; todo dependerá de lo que uno y los demás muestren.

> "*La identidad digital, por tanto, puede ser definida como el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos*

personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital" (INTECO 2012)[5].

«Los menores también poseen una identidad digital», a veces incluso antes de haber usado Internet, fruto de la sociedad que les rodea. Cuántas fotos se suben al día de "*monerías que hace mi niño*", "*la primera vez que mi niña hace*…", "*El quinto cumpleaños de Juan*"… Todo esto se sube a la red y se comparte con amigos y a veces, más veces de las que nos gustaría, con desconocidos.

¿Qué es la huella digital?

La huella digital en Internet es el rastro que se deja en aquellos lugares por los que navega y se va dejando información.

Se debe ser consciente y trasladar a los menores la perdurabilidad de la información en Internet. Es muy sencillo subir fotografías, vídeos, comentarios… a Internet, pero no es tan fácil borrarlos. **«En Internet, las huellas que se dejan son difíciles de borrar».**

RECUERDA: Cuando se publica información en las redes sociales, esta información deja de pertenecer solamente al usuario.

Cuando una información es subida a Internet, se pierde el control sobre ella y no se sabe ni cuándo ni a quién va a llegar. Así, toda la información que se vierte en la red tiene una consecuencia ya sea positiva o negativa. Alguien la leerá y la utilizará y esta información puede ser usada en favor o en contra de la persona.

Por lo tanto, cada vez que se produce un registro en una red o que se suba información se debe valorar qué información se facilitará y cuál será visible para el resto de usuarios. Por eso en el caso de los menores es todavía más importante ser selectivos a la hora de publicar cualquier tipo de información en Internet. Se debe tener en cuenta que la foto más graciosa, traviesa, o el comentario más perspicaz puede no serlo dentro de unos años.

[5] Instituto Nacional de Tecnologías de la Información INTECO. (2012). *Guía para usuarios: identidad digital y reputación online*. [Recurso web: https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/guia_identidad_digital]

¿Qué es la reputación online?

La reputación online es el influjo, estima, prestigio, valoración…de una persona en Internet.

> *"La reputación online es la opinión o consideración social que otros usuarios tienen de la vivencia online de una persona o de una organización".* (INTECO, 2012).

En adolescentes, la reputación online es muy importante pues los y las jóvenes quieren ser respetados y "populares", aunque esta reputación sólo es parcialmente controlable, pues se genera a partir de las opiniones de los demás, lo que hace que se pueda crear "una guerra" para subir en popularidad online. Y esto se agrava cuando el objetivo es generar notoriedad y foro donde se "hable de ti".

Cuidar nuestra imagen o reputación en Internet es cuidar nuestra imagen en nuestra vida real, ya que Internet no es más que una extensión misma de la realidad.

Tal como se ha podido comprobar a lo largo del presente monográfico, la gestión de la privacidad conforma la huella digital que se deja en la red, lo cual, a su vez, da forma a nuestra identidad digital. Esta identidad, observada por los demás, genera nuestra reputación online. Así, a pesar de tratar cada concepto de forma independiente, se ha de tener en cuenta que forman parte de un engranaje al que cuidar en su totalidad.

Publicidad y consumo versus privacidad

No se debe olvidar que detrás de muchos de los diferentes servicios de Internet existe un entramado empresarial, y su base de negocio son los datos que suben los usuarios a la red. Así, la publicidad se ha configurado como un aspecto clave en el ámbito *online*, realizándose gran parte de la inversión en Internet desde el presente sector y apostándose cada vez más en los últimos años por el análisis del comportamiento de los usuarios, rastreando el mismo a través de las *cookies* en el navegador o los identificadores únicos en *smartphones.* Como es sabido, una de las formas en que la

publicidad en Internet se lleva a cabo es a través de las mencionadas *cookies*[6], herramientas que desempeñan un papel esencial para la prestación de numerosos servicios de la sociedad de la información facilitando la navegación del usuario y ofreciendo una publicidad basada en ocasiones en los hábitos de navegación.

Con esta estrategia se pueden lanzar anuncios basándose en la localización del usuario o en páginas web que el usuario haya visitado recientemente. Por lo tanto, debe tenerse en cuenta que la utilización de *cookies* supone la descarga de un archivo o dispositivo en el equipo empleado con la finalidad de almacenar y recuperar datos que se encuentran en el citado equipo, lo cual, además de tener implicaciones importantes en relación con su privacidad, implica que esta información sea importante a la hora de segmentar y ofrecer publicidad atendiendo a nuestros intereses.

En este sentido, existe una reciente preocupación por parte de padres, madres y colectivos vinculados a la protección de menores relacionada con el impacto que puede generar la publicidad sobre los jóvenes y por el exceso de comercialización de la infancia. Por ejemplo, los menores se ven expuestos a productos con implicaciones relacionadas con la salud, tales como la comida rápida o bebidas azucaradas, o que puedan estar expuestos a publicidad sobre productos orientados a un público adulto.

De este modo, la publicidad en Internet representa una forma de exposición de los menores a la publicidad fundamentalmente diferente a la realizada desde la televisión u otros medios debido a su interactividad y a la mayor inmersión de éstos en Internet. Así, podemos diferenciar varios tipos específicos de publicidad online a los que niños y adolescentes se encuentran especialmente expuestos:

- **Publicidad a través de videojuegos (*advergaming*):** publicidad realizada a través de videojuegos creados explícitamente para comunicar y promocionar una marca entre la población infantil y adolescente.

- **Páginas web de marcas:** muchas compañías crean en las páginas web de sus marcas contenidos diseñados específicamente para atraer al público joven e infantil. Normalmente incluyen elementos como juegos, videos, concursos, ofertas, aplicaciones a descargar relacionadas con las marcas, etc.

- **Publicidad a través de las redes sociales tales como Twitter o Facebook.**

[6] "Guía sobre el uso de las Cookies" Agencia Española de Protección de Datos

- **Publicidad a través de móvil:** gracias a la evolución de la telefonía móvil y al elevado uso de los *smartphones* entre la población joven, los niveles de uso de este tipo de publicidad se han visto incrementados, siendo diversas las formas que adoptan los mensajes publicitarios realizados. Así, además de que se pueden emplear todas las técnicas anteriormente desarrolladas, hemos de tener en cuenta que cuando nos descargamos una aplicación determinada, la compañía que la gestiona en muchas ocasiones puede acceder a información sobre nosotros que puede utilizar para enviarnos publicidad.

De este modo, después de décadas de relativa estabilidad en cuanto al uso y desarrollo de la publicidad dirigida a niños y adolescentes, en los últimos años se han podido observar la creación de nuevas vías de publicidad a través de los medios focalizada específicamente al rango de edad que nos ocupa. Por ello resulta necesario que se sigan desarrollando tanto nuevos métodos capaces de cuantificar la exposición de los jóvenes a la publicidad como prácticas que ayuden a los jóvenes a discernir y comprender los intentos persuasivos de este tipo de mensajes.

Privacidad en las APPS (Aplicaciones móviles)

A pesar de que los desarrolladores de aplicaciones para dispositivos móviles persigan el objetivo de ofrecer servicios innovadores y seguros, es necesario tener presente que dichas herramientas (como por ejemplo WhatsApp) pueden plantear importantes riesgos para la vida privada de los usuarios si no cumplen la legislación sobre protección de datos vigente en la actualidad. Por ello, los usuarios tienen el deber y el derecho de poder controlar sus propios datos personales a través de los **consentimientos** oportunos que deban efectuarse en relación al tratamiento de la información en general y de los datos de carácter personal en particular. Es por ello que los responsables de dichas aplicaciones deben informar tanto sobre los datos a recopilar como sobre los usos y finalidades de los mismos. De igual modo resulta necesario aportar información sobre la posible cesión de datos a terceros así como las formas con las que cuenta el usuario para poder revocar su consentimiento inicial y, de este modo, cancelar sus datos.

Así, cuando se utilizan aplicaciones móviles que requieren de un registro previo por parte del usuario o que pueden acceder a información ubicada en el teléfono, se ha de tener en cuenta que en dicho uso se están facilitando datos personales que pueden suponer riesgos para la seguridad y, por consiguiente, para la de aquellos menores

que hagan uso de las mismas. En este caso, uno de los riesgos que se pueden destacar es la **geolocalización** cuya finalidad se orienta a la utilización de información vinculada a una localización geográfica del mundo real[7]. Así, las aplicaciones de geolocalización para dispositivos móviles suelen hacer uso de:

- La **georreferenciación** del propio dispositivo para localizar físicamente un objeto o individuo y acceder a su información específica. Ejemplo de ello sería la utilización de un sistema de navegación mediante GPS o el uso de aplicaciones tal como Facebook Places[8] (aplicación de la red social Facebook que permite compartir la posición del usuario con sus amigos).

- La búsqueda de información y su localización física en un sistema de coordenadas (proceso de **geocodificación**). Un ejemplo de esto sería la utilización de un servicio de mapas para buscar los colegios e institutos de una ciudad.

- La suma de información geográfica a un contenido generado (**geoetiquetado**). Ejemplo de ello sería la creación y publicación en una red social de una fotografía incluyendo las coordenadas del lugar en que fue tomada.

Muchos de los usuarios menores de edad de las aplicaciones móviles no son conscientes de las implicaciones que este tipo de recursos tienen para su propia privacidad. Así, la información referente a la localización es considerada especialmente sensible en el caso de las chicas adolescentes, a pesar de que la mayoría de ellas tienen deshabilitadas este tipo de herramientas al preocuparse por las personas que podrán tener acceso este tipo de información personal[9].

En este sentido, la Agencia Española de Protección de Datos (AEPD) ha participado recientemente en un análisis coordinado para examinar las condiciones de privacidad de las aplicaciones móviles más populares organizado por la Red Global de Control de la Privacidad (GPEN)[10] con el objetivo de fomentar el cumplimiento de la legislación de

[7] Guía sobre seguridad y privacidad de las herramientas de geolocalización. Observatorio de la Seguridad de la Información.
[8] Disponible en: http://www.facebook.com/places/
[9] Report: Teens and Mobile Apps Privacy (2013). Recuperado de http://blogs.law.harvard.edu/youthandmediaalpha/projects/online-privacy/new-report-teens-and-mobile-apps-privacy/.
[10] Resultados del análisis coordinado sobre las condiciones de privacidad de las aplicaciones móviles. Nota de prensa. https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa

protección de datos y privacidad, promover la concienciación de los usuarios y obtener una visión integral y conjunta.

Protección de la privacidad de terceros

Además de prestar atención a la buena gestión de la propia privacidad se ha de ser conscientes del importante papel que de igual modo se desempeña a la hora de gestionar la privacidad de terceras personas por medio de el propio comportamiento online. De este modo, atender y salvaguardar el derecho al honor, a la intimidad y la imagen de terceras personas se configura, así mismo, como responsabilidad de cada persona. Tanto adultos como menores se debe siempre pensar antes de publicar información que no sólo nos pertenece a cada uno, tal como fotos o videos en los que aparezcan otras personas. Aunque especialmente en las redes sociales dispongamos de herramientas para configurar la propia privacidad y determinar con ello quién puede publicar en nuestro perfil o si solicitamos revisar dichas publicaciones de forma previa a su divulgación, el primer paso para la buena gestión de la privacidad de terceros es concienciar sobre los riesgos que pueden darse tras la exposición de la intimidad de cualquier persona sin su exclusivo consentimiento.

Riesgos por la vulneración de la privacidad en los menores

Como es sabido, cuando se realiza un registro en una Web o red social, se ofrece la posibilidad de agregar mucha información sobre la persona, sus gustos, preferencias… y se debe recordar que cualquier información que se ponga en Internet permanecerá mucho tiempo, a veces, para siempre, lo que se ha llamado la huella digital, y si no se configura bien la privacidad, esta información estará a la vista de todo el mundo, cosa que en los menores pueden resultar muy peligrosa.

Así, resultan evidentes los riesgos asociados a la impulsividad que caracteriza a las personas que publican sin pensar en las consecuencias. La información personal que se expone de nosotros mismos y de los demás en la web construye, tal como se ha visto, la identidad de cada uno. Una identidad que puede verse afectada negativamente repercutiendo en nuestra reputación online por una mala gestión de las opciones de privacidad de los servicios y por no meditar ni considerar las consecuencias que comentarios quizá desafortunados o fotografías comprometidas puedan ocasionar en la misma (pudiendo desembocar en un futuro próximo en formas de exclusión social y discriminación, por ejemplo, a nivel laboral).

Uno de los grandes problemas existentes en las Webs de Internet y en las redes sociales es que la configuración de la privacidad suele ser compleja, sobre todo en el caso de niños, niñas y adolescentes y esto hace que afloren peligros para estos pequeños internautas.

Los principales **peligros o riesgos** para los menores asociados a una inapropiada gestión de la privacidad son:

- Publicación por parte del menor de información sensible (imágenes, videos, comentarios) que conlleven un impacto negativo en la construcción de su identidad y reputación. La difusión de imágenes propias de carácter sexual se conoce como *sexting*.
- Uso malintencionado de su información privada por parte de terceros:
    - menores que utilizan imágenes, videos, confesiones…con la intención de hacer daño y atormentar a otros menores, lo que se conoce como *ciberbullying.*
    - adultos que buscan información (gustos, preferencias, hábitos de uso) para establecer lazos de amistad con menores con una finalidad sexual, lo que se denomina como *grooming.* Puede implicar el uso de información sensible (confesiones, imágenes subidas de tono) para extorsionarles y que accedan a sus peticiones.
    - suplantación de la identidad de los menores para cometer fraudes. También puede estar vinculado con los riesgos antes descritos (*ciberbullying* y *grooming*).
- Uso comercial de la información personal (hábitos de navegación, gustos y tendencias) por parte de empresas y agencias de publicidad. Preocupación por el posible desequilibrio de poder entre la sugestión que produce la publicidad y la capacidad crítica de los menores.

Todo esto nos indica que como padres, madres, tutores y educadores de menores de edad hay que informarse y seguir unas pautas para enseñar a nuestros menores y adolescentes a hacer un uso óptimo y adecuado de Internet y gestionar la privacidad en la red lo mejor posible para que tengan una identidad digital adecuada y una buena reputación online.

3. Datos de situación y diagnóstico

Cada vez más, crece la preocupación por la privacidad online, algo que hace unos años no era tan importante, se ha convertido en una de las grandes preocupaciones en el ciberespacio. Un estudio que avala el aumento de la preocupación de las personas con respecto a la privacidad en Internet, es la encuesta realizada por ComRes[11], una consultora de investigación de Gran Bretaña. Esta investigación arrojó que de un total de 10.354 entrevistados que viven en nueve países distintos (Brasil, Gran Bretaña, Alemania, Francia, España, India, Japón, Corea del Sur y Australia), el 79% manifestó estar preocupado por su privacidad en la Red. Asimismo, los países que se mostraron más alarmados por este fenómeno son India (94%), Brasil (90%) y España (90%).

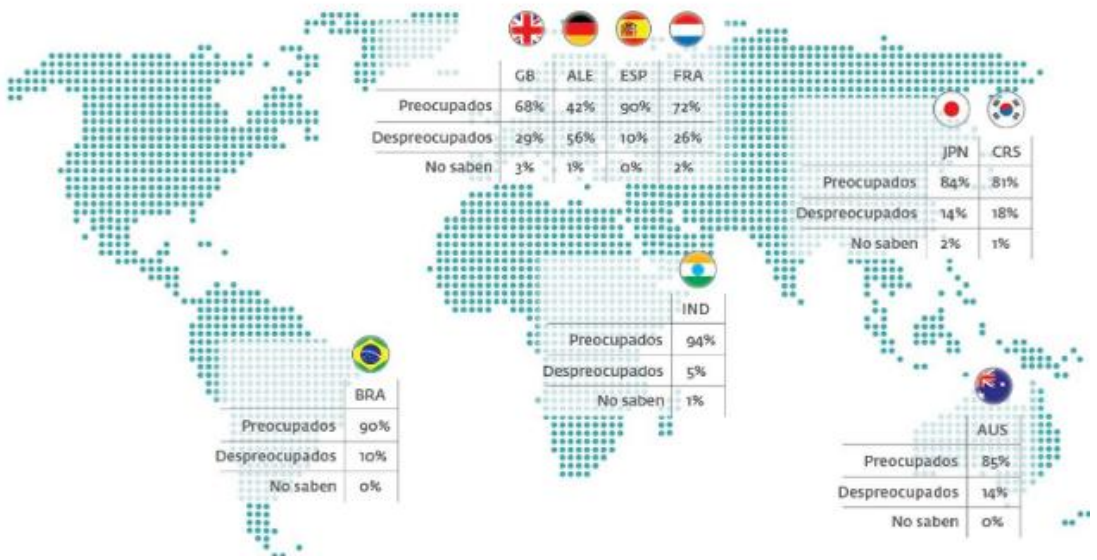

IMAGEN DE INTERNET[12]

A continuación, se muestran los principales hallazgos de la investigación referentes al tema que nos ocupa[13].

La sección española del proyecto EU Kids online[14] ha dado a conocer los resultados de sus estudios sobre la privacidad de los menores en Internet y según sus datos, sólo

[11] ComRes. (2014). *Informe de Privacidad en Internet.* [Resumen] Recuperado de http://comres.co.uk

[12] Recuperado de http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

[13] Equipo de Investigación de ESET Latinoamérica. (2014). *El desafío de la privacidad en Internet.* Recuperado de: http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

[14] Sección española del proyecto EU Kids online. (2011). *Informe EU Kids online.* [Resumen] Recuperado de http://www.ehu.es/es/web/eukidsonline

el 55% de los menores sabe cómo cambiar su configuración de privacidad en las redes sociales. Esto, unido al hecho de que hay un gran número de menores que las están usando por debajo de la edad permitida legalmente, convierte la presencia de menores en este tipo de redes sociales como algo preocupante.

Entre los menores usuarios de redes sociales en España el 67% mantiene su perfil privado (que sólo sus amigos puedan verlo). Este porcentaje es sensiblemente superior a la media europea (43%) lo que supone que los menores españoles en este campo están más concienciados, aunque también podría querer decir que las redes más usadas en España configuran en mayor medida, por omisión, los perfiles como privados.

Un 9% de los menores españoles que usan este tipo de redes sociales publican en ellos información privada como el número de teléfono o la dirección de su domicilio. De media, publican 2'4 datos que podrían permitir identificarles (los anteriormente citados junto a fotos, colegio, edad…).

Sabías que... En España, los menores de 14 años no pueden acceder a las redes sociales, excepto si lo hacen con consentimiento paterno.

A pesar de esto, en España, un 37% de los niños menores de 11 años participa en mundos virtuales, es decir, en comunidades creadas en la Red donde los usuarios o personajes pueden interactuar entre si y usar objetos virtuales. La media en nuestro país está por encima del 23% de los británicos o el 3% de los franceses. El 61% de los niños españoles, el 56% de los británicos y el 12% de los alemanes, de entre 6 y 9 años tenían, en 2012, creado su perfil en Facebook[8].

Por otra parte, y en cuanto a la huella digital, cada vez más la gente quiere hacer uso de nuestro derecho al olvido, es decir, de la facultad que se atribuye a la persona de obtener la eliminación de una determinada información sobre él.

[15] Holloway, D., Green, L. y Livingstone, S. (2013). *Zero to eight. Young children and their internet use*. [Resumen] LSE, London: EU Kids Online.

Según los datos de la Agencia Española de Protección de Datos[16], el número de reclamaciones para cancelar datos personales en la red, han subido de 3 en 2007 a un total de 160 en 2011.

En el caso de los menores es aún más complicado, pues puede ocurrir que parte de su huella digital la hayan creado los adultos antes de que estos pequeños y pequeñas tengan conciencia de ello.

Según datos del estudio elaborado por la EU Kids online, en España, el 71% de los padres y madres han publicado imágenes de sus hijos e hijas menores de 2 años, el 24% de sus hijos recién nacidos y el 24% las ecografías prenatales. Así, estos niños y niñas reciben en herencia una identidad digital que otros han construido para ellos y tienen una huella digital en Internet antes de llegar a la vida.

Del mismo modo encontramos los siguientes datos de niños/as menores de 12 años[17]:

- El 12% que entraban en una sesión de chat utilizaban como Usuario-nick su propio nombre.
- El 8% han facilitado su número de teléfono a través de la red.
- El 12% reconocen haber facilitado su dirección a otra persona.
- El 18% afirman haber acudido a una cita con una persona conocida a través de Internet.

En la misma línea se puede afirmar que el 38% de los niños europeos de entre 9 y 12 años de edad y el 77% de 13 a 16 años tiene un perfil de Facebook. A pesar de que las restricciones de edad son parcialmente eficaces y de las diferencias que se pueden encontrar entre países y redes sociales entre sí, uno de cada cinco niños de 9 a 12 años tienen un perfil en Facebook, llegando a 4 de cada 10 en algunos países[18]. Además, resulta interesante destacar que:

- Los niños más pequeños son más propensos que los mayores a tener su perfil "público".

[16] Agencia Española de Protección de Datos. (2011). *Informe de reclamaciones 2011*. [Resumen] Recuperado de http://www.borrardeinternet.com/wp-content/Huellas-digitales.pdf
[17] Estudio de ACPI- Protégeles para el Defensor del Menor.
[18] Livingstone, Sonia and Ólafsson, Kjartan and Staksrud, Elisabeth (2011) *Social networking, ageand privacy*. EU Kids Online, London, UK.

- Las reglas de los padres para el uso de las redes sociales, cuando se aplican, son parcialmente eficaces, especialmente para los niños más pequeños.

- Una cuarta parte de los usuarios se comunican en línea con personas desconocidas en su vida cotidiana, incluyendo un quinto de usuarios entre 9-12 años de edad.

- Una quinta parte de los niños cuyo perfil es público muestran su dirección y/o número de teléfono (el doble que para las personas con perfiles privados).

La privacidad en el futuro

Según el estudio del *Pew Research Center, The Future of Privacy*[19]*,* en el que se ha consultado a más de 2000 expertos en Internet sobre cómo creen que evolucionará la privacidad en la Red, más de la mitad piensan que seremos personas totalmente públicas para 2025. De este modo, el 55% cree que no se podrá evitar que nuestros datos sean públicos, mientras que el 45% cree que habrá alternativas para que sigamos siendo personas anónimas, todo lo cual dependerá del cuidado que se tenga y de cómo se vele por la privacidad.

En el caso de los menores de edad la situación a la que hacemos referencia se agrava ya que éstos suelen normalmente acceder a la red sin tener en cuenta el peligro, los riesgos o las consecuencias que pueden suponer facilitar sus datos sin contemplar la importancia de la seguridad en cuestiones de privacidad y de la protección de su identidad digital.

Riesgos asociados a una inadecuada gestión de privacidad

Las malas prácticas en la gestión de la privacidad por parte de nuestros menores se configuran como un importante factor de vulnerabilidad para el posible desarrollo de otros riesgos mayores como pueden ser el **ciberacoso, *ciberbullying, grooming*, fraudes o *sexting*.**

¿Cómo se puede saber, si somos padres, madres, tutores y educadores, que los menores a nuestro cargo están siendo víctimas de estos riesgos mencionados, debido a la vulnerabilidad de la privacidad en Internet?

[19] Pew Research Center. (2014). *The Future of Privacy.* [Resumen] Recuperado de http://www.pewresearch.org/

Así, padres, madres y tutores han de tomar conciencia tanto de los riesgos a los que los menores se encuentran expuestos en su relación con las nuevas tecnologías e Internet como de la suma importancia que la correcta gestión de la privacidad alberga como primer paso para reducir la presencia del riesgo. De este modo, existen una serie de conductas significativas que se tendrán que observar y no dejar pasar, pues en la mayoría de los casos los menores tenderán a ocultar las violaciones de su intimidad que hayan podido sufrir en Internet por distintas causas. Según la edad:

En el caso de menores de primaria (6-12 años), que están en una primera fase de conocimiento de Internet, y consideran que el uso de la red es sinónimo de madurez, tienden a ocultar todo tipo de sucesos que le ocurren en Internet, por temor a la prohibición. En esta etapa, los menores tienden a copiar conductas de los mayores y su aprendizaje se basa en el "prueba-error".

En el caso de adolescentes de secundaria (13-17 años), éstos consideran que son mayores y expertos tecnológicos. Comienzan a entrar en redes dónde interactúan más con el mundo virtual tanto conocidos como desconocidos. Buscan experiencias nuevas, retos nuevos que le ayuden a ser "líder tecnológico" entre sus iguales. A pesar de conocer en algunos casos la importancia de la privacidad y seguridad, no son conscientes realmente de su propia vulnerabilidad. Además, Ante cualquier problema tienden a resolverlo solos o piden ayuda a sus iguales antes que a un adulto.

Una apropiada gestión de la privacidad puede llegar a reducir el riesgo de que los menores sufran estos peligros, pues en la mayoría de casos suele configurarse inadecuadamente las opciones de privacidad por parte de la víctima. Por eso es tan importante que como padres, madres o tutores, se insista a los menores sobre la buena configuración de nuestra privacidad en Internet.

Respecto a los educadores en el colegio se debe observar al menor en todos los espacios, es decir, aulas, recreo, biblioteca… para informar al tutor y al equipo directivo del centro, en el momento en que se tenga la simple sospecha de que un chico o chica pueda estar siendo víctima de alguna de estas situaciones. Seguidamente, se deben iniciar las medidas oportunas que marquen tanto el centro escolar como la comunidad educativa para frenar el avance de estos casos. Por ejemplo, en el caso del *ciberbullying*, se deben tomar medidas tanto con el alumnado como con la víctima, actuando de igual modo con las familias de los involucrados,

siguiendo en todo momento los protocolos establecidos para ello (*protocolo de actuación e intervención escolar ante el ciberbullying*[20]).

Lo realmente importante, tanto como padres, madres, tutores o educadores, es la comunicación, no hacerles sentir culpables y trasmitirles en todo momento la confianza necesaria para que el menor pueda apoyarse y contar todo lo ocurrido.

4. Ejemplos de casos reales

A continuación se presentan algunos ejemplos reales obtenidos de periódicos y publicaciones digitales:

Carrefour, multado por exponer la imagen de un menor de edad[21]

> […]
>
> Juan R. C. compró un ordenador portátil en un centro comercial de la citada entidad en Cádiz, pero tras un breve período de uso hubo de devolverlo porque su funcionamiento no era el correcto. Cuando lo hizo, el ordenador contenía fotografías del recurrente, su esposa e hijos menores, pero la entidad comercial le aseguró que borraría las fotografías al formatear el disco duro, cosa que no hizo. «Días más tarde, la entidad demandada expuso el ordenador en un muestrario de informática, enseñando como salvapantallas una foto del recurrente con un hijo menor en la casa familiar», relata la sentencia.
>
> El juzgado de primera instancia condenó a Carrefour a pagar 12.000 euros de indemnización al demandante por vulneración de su derecho a la intimidad, al considerar que sin la autorización de los afectados se había expuesto su imagen con un hijo menor de edad y en su propia casa.

[20] EMICI (Equipo Multidisciplinar de Investigación del Ciberbullying). (2010). *Protocolo de actuación e intervención escolar ante el ciberbullying*. Recuperado de http://www.emici.net/prot/Protocolo%20Ciberbullying.html

[21] EFE Madrid (30 de octubre de 2014) Carrefour, multado por exponer la imagen de un cliente con un hijo menor de edad. *ABC. http://www.abc.es/economia/20141130/abci-supremo-condena-carrefour-foto-201411301222.html*

Expulsado por un mensaje en Facebook[22]

Dos estudiantes fueron expulsados temporalmente, y uno definitivamente, por los mensajes negativos que publicaron en Facebook sobre un profesor. Los estudiantes cursaban séptimo grado (12 o 13 años) en la Chapel Hill Middle School, según My Fox Atlanta. Los niños fueron acusados de transgredir una sección del reglamente de la escuela que supone una infracción de "nivel uno", la peor posible: acusaciones "falsas, tergiversadas, con omisión de información o información errónea" sobre la conducta inadecuada de un empleado de la escuela hacia un estudiante. Alejandra Sosa dijo que lamentaba haber publicado en su estado de Facebook una frase en la que llamaba a su profesor pedófilo. Fue expulsada durante 10 días. Alejandra declaró: "No tenía la intención de arruinar su reputación".

La lección de privacidad de una profesora[23]

¿Hasta dónde puede llegar una foto vuestra en Internet? Esa era el título de la lección que Julie Ann Culp quería impartir a sus alumnos de quinto. La profesora de Tennessee (EEUU) quería aleccionar a su clase sobre los peligros de Internet y sobre cómo viaja la información en la Red.

Para ello, se fotografió con un cartel en el que se leía: "Estoy hablando a mis alumnos de quinto sobre la seguridad en Internet y cómo de rápido una foto puede ser vista por montones de personas. Si estás leyendo esto, por favor, pincha en 'me gusta'. ¡Gracias!"
Seguro que la profe no fue consciente del tsunami que se iba a desatar por culpa de su acción. En apenas seis días, la foto lleva más de 4.200.000 "me gusta" y 100.000 compartidos en Facebook.

Cumpleaños feliz[24]

Thessa, una chica de Hamburgo, Alemania, pensó que solo había invitado a un puñado de amigos a su fiesta de cumpleaños, pero se presentaron unas 1.500 personas, lo que provocó que esta chica de 16 años huyera de casa. Thessa no

[22] Reputación en línea (s.f.) Recuperado de http://www.saferinternet.org/c/document_library/get_file?uuid=154eb773-3936-473f-8fae-5cdddd0261dc&groupId=10137
[23] Porrondo, N. (3 de diciembre de 2013) La lección de privacidad de una profesora. *Yahoo! España. https://es.finance.yahoo.com/blogs/fintechnologiayredeses/lecci-n-privacidad-profesora-viral-002051461.html*
[24] Reputación en línea (s.f.) Recuperado de http://www.saferinternet.org/c/document_library/get_file?uuid=154eb773-3936-473f-8fae-5cdddd0261dc&groupId=10137

comprobó los ajustes de privacidad de su invitación de cumpleaños, por lo que todo el mundo con una cuenta en Facebook tuvo acceso a la invitación.

En los días previos a la fiesta el número de respuestas confirmando la asistencia se disparó a más de 15.000 personas. Eso le dio a la familia de Thessa una idea de lo que se avecinaba. Aunque cancelaron la fiesta y avisaron a la policía, ni siquiera un anuncio público pudo detener a los invitados más persistentes. La noche del cumpleaños de Thessa, grandes multitudes lo celebraron en su ausencia. Durante la noche, once personas fueron detenidas temporalmente y un agente de policía resultó herido.

La Policía detiene a 7 jóvenes por difundir fotos eróticas de una menor de 13 años por Whatsapp[25]

Agentes de la Policía Nacional han detenido a siete jóvenes en Calatayud y Zaragoza por distribuir fotografías eróticas de una menor a través de WhatsApp.

La joven había enviado las imágenes de manera voluntaria y mediante un mensaje privado por una red social a un menor que conoció a través de la red y este las distribuyó entre sus amigos, esta vez sin el consentimiento de la joven, a través de la aplicación de mensajería instantánea para teléfonos móviles. Esto originó una difusión en cadena de las fotografías. Los investigadores centraron sus pesquisas en el entorno de los jóvenes amigos de la víctima y tras varias gestiones lograron identificar, localizar y detener a los siete menores de edad, de entre 14 y 17 años.

5. Estrategias, pautas y recomendaciones para su prevención

Como se ha visto a lo largo del monográfico, la perdida de la privacidad acarrea muchos peligros en los niños, niñas y adolescentes. Por ello, es necesario que todos los agentes implicados en la atención directa a menores trabajen de forma conjunta y transversal con el objetivo de detectar precozmente este tipo de situaciones y poder intervenir lo antes posible.

[25] Asencio, R. (27 de noviembre de 2014) La Policía detiene a 7 jóvenes por difundir fotos eróticas de una menor de 13 años por Whatsapp. *20 minutos.* http://www.20minutos.es/noticia/2309566/0/policia-detiene/foto-erotica/menor-delito/

Es necesario diferenciar entre las estrategias y consejos entre padres, madres, tutores por un lado y educadores por otro pues deben trabajar de manera distinta pero al unísono para evitar la vulneración de la privacidad de los menores a su cargo.

También se tendrá en cuenta los rangos de edad, pues los chicos y chicas de primaria (6-12 años) necesitan sentirse independientes frente al ordenador, pero no solos; necesitan, sin pedirlo, la supervisión y el consejo de los adultos que les rodean. Respecto a los adolescentes de secundaria (13-17 años), necesitan su espacio, pues están creando su personalidad y quieren mayor independencia pero necesitan aprender a tener unos criterios frente a la gestión de su privacidad en Internet.

A continuación se verán algunas **pautas y recomendaciones preventivas**.

Lo primero es el diálogo

Es importante que padres, madres, tutores y educadores a cargo de menores puedan dialogar con éstos sobre qué contenidos subir a la red y cuáles van a ser los criterios de privacidad que aplicarán respecto de la información que suben.

Es necesario conversar pero sobre todo es muy importante hacer partícipe de las decisiones, es decir, permitirles pensar, elegir y determinar por sí mismos, con el consejo de un adulto, cómo y con quién quieren compartir su información.

Es elemental dedicar tiempo a fomentar hábitos correctos en Internet y las redes sociales, al igual que se hace con el aseo y la higiene personal o la lectura. Además es oportuno instalar y hacer uso, siempre que sea posible, de los equipos y aparatos en zonas comunes y establecer unos horarios de uso para evitar el consumo y el uso autónomo y en solitario de Internet, especialmente para los menores de primaria, navegar con ellos y hacerles comprender la trascendencia de intercambiar datos personales y fotografías en Internet son elementos fundamentales. Los menores de secundaria, que tienden a un uso más autónomo, deben saber que pueden conversar con los adultos responsables sobre Internet y deben tener la confianza para contar lo que suelen hacer en la red sin que esto sea una pérdida de intimidad. Es muy importante para los menores sentirse acompañados pero no controlados y vigilados, pues esto puede hacer que se alejan de quienes pueden ayudarlos a resolver sus problemas.

Lo primordial es la creación de un vínculo de confianza que permita un diálogo fluido entre los niños, niñas y adolescentes y sus supervisores online, para que compartan sus preocupaciones e inquietudes y, de ese modo, puedan ayudarlos y ayudarlas a que superen sus dificultades.

El dialogo es fundamental también entre los educadores y los menores. En los centros de enseñanza, los educadores deben, más que imponer, pactar y acordar normas de acceso a Internet y del uso de las áreas de informática con los menores pues así se establece un vínculo de confianza.

Los educadores deben reflexionar junto a los menores sobre los riesgos que conlleva divulgar los datos personales en Internet y deben educar en las buenas prácticas de la privacidad. La buena formación de los menores es vital en estos casos.

El profesorado tiene que facilitar pautas de comportamiento y reiterar al menor que siempre debe dialogar con sus padres o un adulto de confianza sobre las dudas que tenga sobre su privacidad.

Los educadores deben promover charlas con los padres, madres y/o tutores para informar de los peligros que corren sus hijos e hijas si no gestionan bien la intimidad de éstos.

Configurar la privacidad

Por defecto, en la mayoría de Webs donde se registran los adolescentes para subir contenidos como blogs, redes sociales, webs de almacenamiento de archivos… se debe indicar un perfil de protección de la privacidad, es decir, con quien comparto y quien puede ver mi información.

La configuración de la privacidad puede resultar complicada y engorrosa, todo dependerá de la Web y de los parámetros que se quieran o puedan configurar, aunque hay dos perfiles que se encontrarán en casi todas: Público o Privado:

Un perfil público es en el que toda la información es visible por todo usuario.

Un perfil privado es el que sólo comparte la información con las personas que tienen permiso para ello.

El primer paso para proteger la privacidad de los adolescentes es animarlos a que elijan un perfil “privado” explicándoles los riesgos que podría tener si sus datos son públicos.

En el caso de los menores de 14 años, como se ha visto, no pueden dar sus datos ni registrarse en estas Webs, excepto si lo hacen con consentimiento paterno. En este caso, el padre, madre o tutor que da el permiso configuraría la privacidad para así proteger los datos de sus menores de primaria.

Se debe hacer hincapié a los adolescentes a que lean las condiciones de uso y la política de privacidad de los sitios que visitan, pues los mejores sitios explican muy bien la información que recogen y las condiciones de uso. Enseñar a configurar las opciones de privacidad es importante, pero lo fundamental es ayudar a conocer cómo funcionan y los efectos posibles de una mala configuración así como las limitaciones de estas opciones.

Se pueden utilizar dos páginas de referencia para obtener información sobre como configurar la privacidad en cada una de las redes sociales más utilizadas en España:

La página de la Oficina de Seguridad del Internauta:

https://www.osi.es/es/redes-sociales

La página publicada por Save the Children bajo el nombre "De aquí no pasas":

http://www.deaquinopasas.org/

Seleccionar los contactos

Si nuestros menores han optado por un perfil privado, ahora deben decidir a quién permitirán ver su perfil. La labor tanto de padres, madres y tutores, como la de los educadores, será la de aconsejar que solo acepten como amigos a contactos que conozcan en la vida real y que sepan ciertamente que la persona a la que están aceptando es la que dice ser y no ha usurpado su identidad. Para ello pueden contactar previamente con la persona que le ha enviado la invitación de amistad (llamándola por teléfono o mandándole un mensaje privado solicitándole que le mande una foto) para cerciorarse de la identidad de ésta. Se puede explicar a los menores

que si se encuentran con un contacto que no desean o no conocen, siempre es mejor bloquear el acceso de esa persona a su cuenta por precaución.

Es una gran labor hacer entender a los menores que deben diferenciar muy bien entre amigos y contactos. Hacer un contacto sólo requiere un clic, en cambio, una amistad se crea a lo largo de mucho tiempo.

El estudio que realizó UNICEF[26] sobre amistad virtual, mostró que el contacto con los amigos a través de Facebook es la motivación principal para su uso: amigos que ya se tienen, amigos que se recuperan, conocidos que se frecuentan poco en forma personal. Esto significa que los amigos virtuales quedan en segundo lugar, porque el gran atractivo es enterarse de lo que hacen los amigos que ya se tienen, facilitar los encuentros sociales con ellos y también intercambiar opiniones y sentimientos personales.

De todos modos, es indispensable prestar atención a las amistades virtuales de los y las adolescentes y siempre recordarles que no deben citarse en persona con estas ciber-amistades.

Revisar los ajustes periódicamente

Es demasiado frecuente que los menores se equivoquen y ubiquen en lugar erróneo alguna información en las Webs o que publiquen algo que quieren que sea privado en una parte pública. Como responsables de ellos, se debe insistirles, que revisen sus políticas de privacidad periódicamente y que comprueben qué información están compartiendo con los demás. Muchas redes sociales ofrecen la opción de comprobar los “ajustes de seguridad” permitiendo a sus usuarios que vean su propio perfil como si fueran otra persona. De esta manera, pueden ver con claridad si se muestra en su perfil alguna información que no desea que aparezca y así poder modificar la privacidad.

Los tutores y educadores tiene la obligación, tanto en la casa como en el aula, a recordar a los chicos y chicas que cada vez que publiquen deben comprobar que no alteran la política de privacidad y que lo que quieren que sea privado no lo pongan

[26] Weich, J, Weinbaum, E y Weinbaum S. (2011) *Internet Segura.* Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo y UNICEF. Recuperado de http://www.unicef.org/argentina/spanish/Unicef_InternetSegura_web.pdf

público, pues cuando se sube algo, ya sea una imagen un vídeo o texto, se puede modificar el público que puede tener acceso a esos datos.

Examinar lo que otros publican

Como madres, padres o tutores, cuidar la información que los menores a su cargo publican en las redes sociales no es lo único que hay que hacer para una buena gestión de la privacidad, pues otras personas pueden publicar imágenes y vídeos y enlazar el nombre de sus hijos a estos contenidos sin su autorización paterna, si su hijo/a es menor de 14 años, o sin el permiso del adolescente (mayor de 14 años). Es muy común que este etiquetado, que es como se denomina esta acción, se realice de manera inconsciente, negligente, compulsiva o incluso temeraria pero hay que explicar a nuestros jóvenes que la mayoría de redes sociales existentes permiten a sus usuarios desactivar la función de etiquetado, o poseen la opción de que se solicite la conformidad del usuario para cada contenido que se desee etiquetar. Esa será la gran labor, recomendar a los menores a su cargo que configuren esta opción para que puedan mantener el control sobre su reputación en Internet, además de explicar que deben informar a los demás del respeto por su privacidad y si hay algo que les molesta, que traten de reaccionar de manera calmada y no violenta y si no se resuelve con el diálogo, ejercer su derechos.

Los educadores, deben tratar este tema de la privacidad de otras personas en el aula y ser muy perseverantes, explicando el peligro de los etiquetados de terceras personas sin su consentimiento, siendo un acto denunciable, y enseñar que derechos tiene cada niño o niña respecto a su privacidad.

Desde el centro escolar, se tiene que comunicar al alumnado las responsabilidades civiles, administrativas o penales cuando se vulneran los derechos, como el del honor, la intimidad personal y familiar y la propia imagen, tanto propios como de terceros en Internet.

Proteger la información delicada

Es importante hablar con los menores para que entiendan los peligros que pueden correr si comparten con extraños información de carácter personal, número de teléfono, la localización, las contraseñas, cuentas de correo electrónico, datos bancarios, dónde les gusta ir a jugar… Se debe hacer saber que estos datos pueden

ser luego empleados con el propósito de provocar daños o realizar estafas y secuestros, entre otras conductas delictivas.

En Internet existen muchas páginas que ofrecen servicios que pueden parecer interesantes sólo a cambio de un registro rellenando un formulario. Muchas páginas Web piden datos personales, pero hay que saber que la ley les obliga, antes de facilitar estos datos, a que digan quiénes son ellos, qué datos necesitan y para qué los van a utilizar. Las redes sociales buscan negocio explotando la información, gustos y motivaciones de sus usuarios, ya que utilizan estos datos para seleccionar publicidad y ganar dinero de las empresas anunciantes.

La red está llena de estafas así que hay que enseñar a los menores a que desconfíen y tengan cuidado con anuncios de negocios que son demasiado buenos para ser reales, avisos de empleos falsos, avisos de que ha ganado la lotería, solicitudes de ayudar a un extraño en un lugar distante a transferir fondos, chollos de última hora… Todas estas estafas pretenden apoderarse de datos o de dinero de una forma rápida y engañosa así que se debe enseñar a nuestros menores a detectarlos y sobre todo a crear un hábito de preguntar a un adulto antes de caer en las redes de estas informaciones tan llamativas.

En los centros educativos se debe enseñar a los menores cuáles son sus derechos frente a sus datos personales y cómo pueden ejercer los mismos. Los educadores deben dialogar con los adolescentes para que sean conscientes de la peligrosidad de revelar los datos a desconocidos, como no lo harían en la vida real. En el centro escolar, se tiene que informar al alumnado las responsabilidades civiles, administrativas o penales cuando se vulneran el **«derecho fundamental a la protección de datos de carácter personal»**, tanto propios como de terceros en la red.

Predicar con el ejemplo

Se debe enseñar a los menores a predicar con el ejemplo, a ponerse en la piel de otras personas y a no hacer lo que no les gustaría que les hicieran a ellos y ellas. Se deben crear hábitos como pedir permisos antes de etiquetar fotografías subidas por otras personas o antes de subir contenido y etiquetar a otras personas. Se debe hacer ver que es importante preguntarse qué información de otras personas se está

exponiendo y asegurarse que no les importa. No hay que olvidar que la persona que sale en la una foto es dueña de su imagen.

En definitiva, una imagen o video de otra persona debe ser tratada como un dato personal que no podemos publicar sin su autorización previa.

Hay que recordar que los menores de 14 años no pueden dar dicha autorización, por lo que sería necesario pedir autorización a sus padres. Así, para publicar imágenes o videos de menores se necesita el permiso de ambos padres (o tutores legales), por escrito. Según la ley de protección de datos, este consentimiento para la publicación de las imágenes ha de ser libre, previo e informado, específico y revocable.

Controlar desde dónde y cómo conectarse

Existen en el mercado un variado catálogo de dispositivos móviles como tabletas, *smartphones*, o portátiles que se usan a diario sin recordar que en ellos se almacenan gran cantidad de información privada: fotos y vídeos, correos electrónicos, contactos, acceso a redes sociales, datos de pago online, etc. Estos dispositivos, cada vez más, están siendo usados por menores, bien de uso exclusivo por y para ellos y ellas o bien de uso compartido en la unidad familiar, centros escolares, centros públicos…

Estos dispositivos pueden ser un punto crítico de la privacidad de niños, niñas y adolescentes que los usan. Si alguien accede a toda esta información puede hacer un mal uso de ella e incluso podrá hacerse pasar por estos menores en Internet para obtener datos de familiares y amigos. Es por eso que se debe enseñar a los menores a proteger la información que se almacena en estos dispositivos frente a posibles pérdidas o robos, si el aparato nos pertenece, o si no, instruirles a que nunca deben dejar contenido personal en ellos. Si el acceso se hace desde centros escolares, el profesorado debe hacer recomendaciones tales como: siempre cerrar las sesiones iniciadas, borrar los datos personales que se hayan usado en la misma o que se hayan almacenado en el equipo (como por ejemplo, contraseñas guardadas en el navegador).

Es importante que se configuren y establezcan modos de acceso seguros mediante contraseñas, lo que ayudará a proteger la información. En el caso de los menores de primaria, como adultos responsables de ellos se debe ayudarles para realizar esta acción, mientras que en el caso de los adolescentes de secundaria, si ya poseen esos

conocimientos, los adultos deben insistir en que los usen, y si no los tienen, nuestro deber es ayudarles al igual que a los menores de primaria.

En ocasiones nuestros pequeños y pequeñas usan redes WIFI abiertas o públicas en lugares como aeropuertos, cafeterías, centros comerciales, hoteles… a las que se pueden conectar junto con otras muchas personas a las que no conocen y es por eso que los adultos tienen que concienciar a los menores a evitar el envío de información personal en estas redes pues pueden existir personas, con suficientes conocimientos técnicos, que pueden conectarse a la misma red y capturar lo que enviamos, incluso las contraseñas, para posteriormente usarlo de manera dañina o fraudulenta contra nuestros menores.

Otros consejos para cuidar la privacidad en Internet de los menores

Los encargados de la seguridad, tanto en casa como en el colegio, deben seguir ciertas recomendaciones como instalar un antivirus y actualizarlo periódicamente, poner un antiespia o *antispyware* que ayude a eliminar los programas espías o troyanos que puedan entrar a través de distintas páginas, actualizar el sistema operativo y las aplicaciones instaladas activando para ello las actualizaciones automáticas para evitar que a través de un fallo de seguridad del mismo alguien se pueda apoderar de datos del ordenador…

Otros consejos que los adultos pueden dar a los menores son:

- No entrar en páginas Web sospechosas.
- No facilitar las contraseñas a nadie y modificarlas periódicamente.
- En el uso del correo electrónico, cuando se mande una misma información a varios contactos se debe usar el CCO (correo con copia oculta) para no mostrar los contactos a los demás destinatarios.
- Realizar transacciones comerciales en páginas Web seguras, es decir, deben tener una "s" después del http (http**s**//www.seguro.es).
- Controlar el uso de la Webcams y cuando no estén en uso, taparlas o quitarlas pues pueden ser encendidas por control remoto sin darnos cuenta.

- No compartir libremente los datos de geolocalización pues todos sabrán dónde estás y dónde no.

También señalar que los centros educativos tienen la posibilidad de participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**[27], que pretende potenciar actuaciones preventivas en relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros. En el marco de este Plan los miembros de las Fuerzas y Cuerpos de Seguridad realizan charlas, visitas y actividades en centros escolares, dirigidas tanto al alumnado como al resto de la comunidad educativa (directivos, personal docente y Asociaciones de Madres y Padres de Alumnos). Como medidas adicionales, se contemplan acciones de sensibilización y formación dirigidas a concienciar sobre el "uso responsable de las nuevas tecnologías y los riesgos que las mismas pueden implicar, promoviendo, a su vez, la comunicación a su entorno familiar, educativo o a las Fuerzas de Seguridad de los hechos de los que pueden ser víctimas o testigos.

6. Mecanismos de respuesta y soporte ante un incidente

En muchos casos, la vulneración del derecho a la intimidad o privacidad de cualquier persona podría ser constitutivo de distintos tipos de delitos como pueden ser descubrimiento y revelación de secretos, injurias, falsedad en documento privado, estafas, etc.

Información para padres, madres y tutores en caso de vulneración de intimidad o privacidad de menores en la red

En caso de detectar algún tipo de vulneración de intimidad o privacidad de menores (por ejemplo, una foto/vídeo privado o dato de carácter personal en Internet que se ha publicado sin nuestro consentimiento -en caso de menores de 14 años- o sin el consentimiento del menor -si es mayor de 14-, y no es por un error de algún conocido), en primer lugar deberíamos comunicárselo a la persona implicada y pedirle la retirada

[27] Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

de la imagen. De no ser esto posible, el camino que se debe seguir como padre, madre y/o tutor sería:

1. Guardar pruebas de los hechos o de las evidencias electrónicas imprimiendo pantallazos, grabando la información en pen-drive, tomando imagen de la pantalla mediante una cámara fotográfica o un móvil, donde aparezcan fechadas las fotografías…

2. Ponerse en contacto con los administradores del portal o red social para solicitar su retirada junto con los comentarios ocasionados. Si las webs no lo eliminan serían responsables de un hecho delictivo, incluso si el contenido ilícito lo ha subido un usuario particular de dicho portal o red social. Redes sociales como Facebook o Tuenti y portales como YouTube cuentan con mecanismos para que los soliciten la supresión de fotos o vídeos que violan su intimidad junto a las imágenes y vídeos.

   Por ejemplo, para obtener más información sobre cómo denunciar contenido en facebook (sobre publicaciones, fotografías o fotos) accede al siguiente enlace:

   https://es-es.facebook.com/help/181495968648557/

3. Ponerse en contacto con los posibles buscadores que hayan indexado los contenidos solicitando su bloqueo o retirada.

4. Denunciar ante la Agencia Española de Protección de Datos: www.aepd.es.

5. Presentar una denuncia ante la Policía o la Guardia Civil. En las webs www.policia.es y www.guardiacivil.org podemos poner la denuncia.

Información para educadores en caso de vulneración de intimidad o privacidad de menores en la red

Si los educadores detectan o son informados por los propios menores o amistades, que se han vulnerado la intimidad o privacidad de un menor en la red, además de observar al menor en todos los ámbitos posibles (aula, patio, biblioteca…), el protocolo que deben seguir es básicamente el siguiente:

1. Poner el caso en conocimiento del tutor y del equipo directivo por escrito, cuidando la confidencialidad.

2. Poner en conocimiento de los padres o tutores el incidente detectado para que estos sigan el protocolo oportuno.

En caso de ver indicios de que los menores puedan ser víctimas de otros peligros o riesgos como el *ciberbullying*, *sexting*, *grooming*… en el ámbito educativo, se seguirán los protocolos, para este tipo de delitos, que marque la comunidad educativa y que el profesional debe conocer.

7. Marco legislativo aplicable a nivel nacional y europeo.

El derecho a la intimidad personal y familiar, al honor y a la propia imagen, es inherente a toda persona, inalienable y concreta el valor de la dignidad humana en el Estado social y democrático de derecho.

La normativa legal que se aplica en temas de privacidad de los menores son:

La Constitución Española de 1978 al enumerar, en el capítulo III del Título I, los principios rectores de la política social y económica, hace mención en primer lugar a la obligación de los Poderes Públicos de asegurar la protección social, económica y jurídica de la familia y dentro de ésta, con carácter singular, la de los menores. Además, La Constitución, en su artículo 18.4 dispone que *"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"* aquí también se incluyen a los menores.

La Convención de Derechos del Niño, de Naciones Unidas, de 20 de noviembre de 1989, ratificada por España el 30 de noviembre de 1990, garantiza a cada niño, niña y adolescente el derecho a opinar y ser escuchado (art. 12), la libertad de expresión, incluida la libertad de buscar, recibir y difundir información (Art.13), la libertad de asociación y asamblea y el derecho a la información (artículo 17), entre otros.

Otras leyes españolas, que protegen la difusión de las imágenes de los menores son la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, la Ley Orgánica 1/1996, de protección jurídica del menor y la última instrucción 2/2006 sobre el Fiscal y la Protección del Derecho al Honor, Intimidad y propia imagen de los menores, que prohíben la difusión de datos o imágenes referidos a menores de edad cuando sea contrario a su interés, incluso cuando conste el consentimiento del menor.

La Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico, recientemente modificada por la Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información, normativa básica para la regulación de servicios prestados a través de sitios Web, contempla una mayor protección de los derechos de la infancia, ya que los menores de edad son considerados como especialmente vulnerables.

Con el objetivo de proteger y salvaguardar los derechos de los consumidores y usuarios ante las comunicaciones comerciales difundidas por vía electrónica la Unión Europea modificó, en 2009, la Directiva 2002/58 sobre privacidad y comunicaciones electrónicas para hacerla más restrictiva e incluir nuevas exigencias. Finalmente, estas modificaciones han sido incorporadas a la legislación española mediante el Real Decreto 13/2012, de 30 de marzo, que modifica los artículos 20, 21 y 22 de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI) que regulan la publicidad difundida por vía electrónica.

El apartado segundo del artículo 22 de la LSSI establece:

2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

La Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, también protege los datos personales de los menores.

Los derechos para proteger los datos personales de cualquier persona, mayor o menor de edad, se conocen como derechos "ARCO"; derechos a Acceso, Rectificación, Cancelación y Oposición.

La LOPD establece que los datos personales de los menores de 14 años sólo pueden ser tratados por terceras personas con el consentimiento de los padres o tutor legal.

¿Cómo borrar las huellas digitales?

Con respecto a la huella digital del menor en Internet, borrarla es uno de los grandes problemas, es lo que se llama el derecho al olvido.

El Boletín Oficial del Estado ha publicado, el pasado mes de noviembre de 2014, el Código del Derecho al Olvido[28]. Con esta publicación los ciudadanos podrán saber qué actuaciones deben llevar a cabo para eliminar información**,** datos personales de Internet y saber en qué condiciones tienen derecho a desaparecer de la red. En el punto número 29 del Código del Derecho al olvido, se podrá leer todo lo referido a los menores.

A nivel europeo

En la legislación europea[29], la protección de los menores en relación con los riesgos relacionados con la vulneración de la privacidad e intimidad en el ámbito digital, partimos de la Carta Europea de los Derechos del Niño y del Libro Verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información (1996). A raíz de este último, nació la Recomendación 98/560/CE del Consejo, de 24 de septiembre de 1998, relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo

[28] Boletín Oficial del Estado (3 diciembre de 2014), *Código del Derecho al Olvido*. Recuperado de http://www.boe.es/legislacio/codigos/codigo.php?id=094_Codigo_del_Derecho__al_Olvido.pdf

[29] Síntesis de la Legislación de la UE (s.f.), *Código del Derecho al Olvido*. Recuperado de http://europa.eu/legislation_summaries/

de los menores y de la dignidad humana. Completando y actualizando la Recomendación anterior y teniendo en cuenta la evolución tecnológica nace la Recomendación 2006/952/CE del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativa a la protección de los menores y de la dignidad humana y al derecho de réplica en relación con la competitividad de la industria europea de servicios audiovisuales y de información en línea. La Recomendación invita a los Estados miembros a emprender acciones que permitan a los menores utilizar de manera responsable los servicios audiovisuales y de información en línea. Dicha responsabilidad puede obtenerse mediante una mayor sensibilización de los padres, profesores y formadores ante el potencial de los nuevos servicios y de los medios disponibles para la protección de los menores.

Respecto a la protección de datos, actualmente, existe el borrador del futuro reglamento europeo de protección de datos que debe estar listo para 2016 y se empezará a aplicar en el primer semestre de 2018.

Otra normativa que defiende los derechos de los menores es la **Resolución de 27 de febrero de 1996 del Consejo de Telecomunicaciones para impedir la difusión de contenidos ilícitos de Internet, especialmente la pornografía infantil.** Propone medidas para intensificar la colaboración entre los Estados miembros independientemente de que cada uno de ellos aplique la legislación que exista en su país sobre la materia.

Otras directivas europeas en materia de seguridad informática, que también regulan la privacidad son:

Directiva 2009/136/CE/ del Parlamento Europeo y del Consejo, de 25 de noviembre , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre, por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y

a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

8. Organismos, entidades y foros de referencia

A continuación se presentan una serie de organismos y entidades de referencia en materia de gestión de la privacidad e identidad digital:

ORGANISMO / DETALLE
Chaval.es (www.chaval.es) Iniciativa del Ministerio de Industria, Energía y Turismo, puesta en marcha por Red.es para responder a la necesidad de salvar la brecha digital entre padres, madres, tutores y educadores respecto al avance de los menores y jóvenes en el uso de las TIC. Ofrece recursos de sensibilización y formación sobre la gestión de la privacidad.
Oficina de Seguridad del Internauta (www.osi.es) Proporciona información y soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.
Pantallas Amigas (www.pantallasamigas.net) Iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Algunas de sus actividades principales son la creación de recursos didácticos, sesiones y jornadas formativas y estudios, con especial énfasis en la prevención del ciberbullying, el grooming, el sexting, la sextorsión y la protección de la privacidad en las redes sociales. Dispone de una línea de ayuda para niños y adolescentes ante situaciones de peligro en Internet.
Agencia Española de Protección de Datos (www.agpd.es) Vela por el cumplimiento de la legislación sobre protección de datos y controla su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos
Instituto Nacional de Ciberseguridad (www.incibe.es) Sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI). Es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores

estratégicos.

9. Más información

Se presenta a continuación una relación de documentos y recursos para ampliar información sobre *gestión de la privacidad e identidad digital*:

RECURSO / DETALLE
Guía para usuarios sobre identidad digital y reputación online (INTECO) Guía que analiza los conceptos de identidad digital y reputación online desde el punto de vista de la privacidad y la seguridad. Nos describe situaciones que preocupan a los usuarios, como la suplantación de identidad, las amenazas a la privacidad o los impactos derivados de publicaciones falsas o descontextualizadas. Asimismo, analiza las implicaciones jurídicas de estas categorías de riesgo y se aportan una serie de pautas de actuación. www.incibe.es
Cuida tu imagen online Se trata de un recurso educativo online sobre cuestiones relativas al manejo en Internet y con la telefonía móvil de la imagen y la privacidad por parte de niños, niñas y adolescentes. www.cuidatuimagenonline.com
Protección de la privacidad Portal web de sensibilización y formación para la protección de la privacidad y los datos personales en redes sociales y smartphones. Aportan también una serie de recursos didácticos. www.proteccionprivacidad.com
Simulador de privacidad Este recurso ayuda a entender que la privacidad de uno no depende solamente de uno mismo y la importancia de proteger la privacidad de terceros que aparecen en las imágenes. www.simuladordeprivacidad.com

e-Legales

Portal web de referencia e información complementaria para todos los asuntos relacionados con los delitos cometidos por medio de las TIC, principalmente Internet y telefonía móvil. En él nos dan a conocer algunos conceptos necesarios y para estar al día sobre las últimas noticias relacionadas.

www.e-legales.net

De aquí no pasas

Aquí encontrarás toda la ayuda para la configuración de privacidad de las principales Redes Sociales de Internet.

www.deaquinopasas.org

10. Bibliografía

Agencia Española de Protección de Datos. (2011). *Informe de reclamaciones 2011.* Recuperado de http://www.borrardeinternet.com/wp-content/Huellas-digitales.pdf

Boletín Oficial del Estado (3 diciembre de 2014), *Código del Derecho al Olvido.* Recuperado de http://www.boe.es/legislacion/codigos/codigo.php?id=094_Codigo_del_Derecho_al_Olvido.pdf

ComRes. (2014). *Informe de Privacidad en Internet*. Recuperado de http://comres.co.uk

Elvira Mifsud. (2012). *Introducción a la seguridad informática. Seguridad de la información/Seguridad informática.* Creative Commons.

EMICI (Equipo Multidisciplinar de Investigación del Ciberbullying). (2010). *Protocolo de actuación e intervención escolar ante el ciberbullying*. Recuperado de http://www.emici.net/prot/Protocolo%20Ciberbullying.html

Equipo de Investigación de ESET Latinoamérica. (2014). *El desafío de la privacidad en Internet.* Recuperado de:http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

Guía sobre el uso de las Cookies. Agencia Española de Protección de Datos

Guía sobre seguridad y privacidad de las herramientas de geolocalización. Observatorio de la Seguridad de la Información.

Holloway,D., Green, L. y Livingstone, S. (2013). *Zero to eight. Young children and their internet use.* LSE, London: EU Kids Online.

Instituto Nacional de Tecnologías de la Comunicación INTECO. (s.f) *Guías legales La privacidad en Internet.*

Instituto Nacional de Tecnologías de la Información INTECO. (2012). *Guía para usuarios: identidad digital y reputación online.*

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE nº 298 de 14 de diciembre de 1999.

Livingstone, Sonia and Ólafsson, Kjartan and Staksrud, Elisabeth (2011) Social networking, ageand privacy. EU Kids Online, London, UK.

Pew Research Center. (2014). *The Future of Privacy.* [Resumen] Recuperado de http://www.pewresearch.org/

Real Academia Española. (2001). *Diccionario de la lengua española* (22.ª ed.). Consultado en http://www.rae.es/recursos/diccionarios/drae

Report: Teens and Mobile Apps Privacy (2013). Recuperado de http://blogs.law.harvard.edu/youthandmediaalpha/projects/online-privacy/new-report-teens-and-mobile-apps-privacy/.

Resultados del análisis coordinado sobre las condiciones de privacidad de las aplicaciones móviles. Nota de prensa. https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa

Sección española del proyecto EU Kids online. (2011). *Informe EU Kids online*. Recuperado de http://www.ehu.es/es/web/eukidsonline

Síntesis de la Legislación de la UE. (s.f.). Código del Derecho al Olvido. Recuperado de http://europa.eu/legislation_summaries/

Weich, J, Weinbaum, E y Weinbaum S. (2011). *Internet Segura*. Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (inadi) y UNICEF.

Referencias web:

Privacidad online.

http://www.privacidad-online.net

Pantallas Amigas.

http://www.pantallasamigas.net

Portal del menor.

http://www.portaldelmenor.es

Safer Internet.

http://www.saferinternet.org

Facebook Places.

http://www.facebook.com/places/