1.1

Identidad digital y gestión de la privacidad

Juan García Cortés 2019
garcia_juacor@gva.es
@juan_garciaTIC

Índice

1. Introducción

El uso intensivo por parte de todos de las tecnologías de la información nos plantea nuevos retos de gestión de la información y de su privacidad. A lo largo de los años se ha producido una considerable evolución, desde la web 1.0 que nos mostraba páginas web estáticas sin posibilidad de interacción hasta la web 2.0 donde se introdujo el concepto de compartir y colaborar.

Esta posibilidad de creación de contenido, ha posibilitado la utilización de herramientas tan utilizadas hoy en día como blogs, wikis, servicios de videostreaming o redes sociales. En definitiva, colaboramos, compartimos e interactuamos con los demás en Internet.

Esta forma de interactuar y compartir genera comunidades virtuales donde la información circula rápidamente en la red y como consecuencia aparece el riesgo de que esa información pueda llegar a donde no queremos o recibirla sin quererla.

Debemos por tanto, pensar que esta evolución que proporciona un gran avance que nos permite crear, compartir y mostrar contenido conlleva unos riesgos con los que tenemos que convivir cuidando nuestra privacidad y nuestra identidad digital.

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

2. ¿Qué es la privacidad?

Seguramente todos estaremos pensando en una definición de este estilo:

> **Privacidad**: "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". (RAE, 2001)

Si a esta definición le añadimos Internet tendremos que hablar de la **Privacidad en Internet** y con ello deberemos de hablar del **control de la información personal que posee un usuario que se conecta a Internet.**

2.1. ¿Por qué es importante que gestionemos bien nuestra privacidad?

Nuestra privacidad es "un tesoro" que se comparte en mayor o menor medida con nuestra familia, nuestros amigos, etc. en definitiva con los más cercanos. No la compartimos con personas desconocidas o con aquellas que no sean de nuestra confianza. No damos nuestros datos personales: nombre, dirección, ... a cualquiera por la calle pero cuando estamos conectado lo hacemos continuamente.

Debemos realizar una buena gestión de la privacidad par evitar problemas y estafas porque a parte de los datos personales que hemos mencionado anteriormente, estos datos nos determinan como persona en la red: nuestras aficiones, gustos, intereses o creencias. Toda esta información puede ser usada de forma inadecuada.

Por tanto, cuando hablamos de protección de datos personales tenemos que tener presente:

- Información que identifica a la persona. Nombre, dirección, etc.
- Información que puede hacer identificable a una persona. Información que habla de ella misma.

Gestionar la privacidad no sólo significa gestionar los datos personales también debemos “cuidar” de aquella información que habla sobre las preferencias, gustos, comentarios, ideas, etc.

- Son datos personales: el nombre y apellidos, el DNI, una fotografía, la dirección, el número de teléfono, la voz...
- También sin datos personales los que 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.

En este sentido todo lo que realizamos, compartimos, comentamos influye tanto en nosotros como en otras personas. Esto nos lleva ha hablar de otro concepto: la **identidad digital**. Todo influye de forma directa o indirecta y negativa o positiva en la creación la identidad digital y reputación personal.

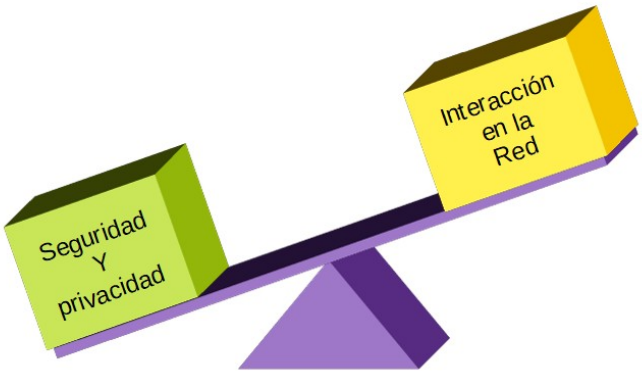
Se debe concienciar sobre la importancia de “pensar antes de publicar” sobre todo en los menores. Pensar en las posibles consecuencias que pueda tener en un futuro lo que en el presente exponemos de nosotros mismos. Saber gestionar correctamente nuestra privacidad es fundamental para construir una identidad digital sana y una buena reputación que no nos condicione ni en el presente ni en el futuro.

Si nos referimos a los menores, esto es de vital importancia. Un mal paso puede definir su identidad digital futura. Son más vulnerables, impulsivos, etc..

La falta de privacidad en Internet es una realidad que cambia las vidas de todos, creando víctimas y teniendo consecuencias muy graves en personas que, sin saberlo, han hecho de su vida algo público. Por tanto, conceptos de ciudadanía y vida social han cambiado en la era digital, se utiliza mucho más comunicaciones públicas que privadas. Hablamos de esa “existencia online” donde las personas publican contenidos públicos que

podrán ser compartidos a su vez por otros usuarios, consiguiendo formar parte de grupos o comunidades y para ello saltando en ciertas ocasiones su propia seguridad.

El reto está en mantener en **equilibrio la seguridad y privacidad** con la interacción en la red.



A continuación vamos a ver algunos de los conceptos que nos ayuden a definir la seguridad en la red:

- **Confidencialidad. L**a información sólo podrá ser accesible a aquellas entidades o personas autorizadas por el usuario. En las redes sociales es especialmente importante 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.

Debemos tener presente estos conceptos o estándares, como punto de partida para mantener la privacidad y la seguridad en la red. La Ley de Protección de Datos (LOPD) en su día y actualmente el Reglamento General de Protección de Datos (RGPD) son de vital importancia dentro del ámbito de las nuevas tecnologías, asegurando que no se produzca divulgación ilícita ni uso indebido de información privada de los usuarios. Más adelante veremos un breve resumen de cada una de las normas y qué novedades aporta el RGPD.

Además de estos conceptos debemos tener presente, desde el punto de vista de velar por nuestra privacidad, cómo vamos a movernos en el contexto de Internet:

- **Privacidad y anonimato de la identidad digital**

  Podemos actuar bajo un “nick”. Este “nick” no es más que una palabra, nombre, sobrenombre, alias o pseudónimo que utiliza un usuario en los medios digitales para identificarse y poder comunicarse. Algunos sitios nos permitirán esto y otros no. Debemos valorar esto considerando, nuestro entorno, uso y tipo de interacción ya que esto influirá en la identidad digital y en la interacción con el resto de usuarios de la red.

  Por ejemplo, si nos encontramos en una red profesional como LinkedIn, sería interesante y necesario utilizar nuestros datos reales en otro caso tal vez no.

- **Privacidad de nuestros datos personales**

  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 según a qué usuarios vamos a dar acceso a los mismos. Es muy recomendable configurar la privacidad al máximo en un principio para poco a poco, después de familiarizarnos con la plataforma, ir compartiendo nuestros datos.

A modo de resumen podemos decir que, al igual que aplicamos pautas de seguridad y privacidad en nuestra vida real, la privacidad ha de estar presente cada vez que interaccionamos en la red. Es importantísimo asumir esta necesidad y aprender a aplicar sus bases en nuestro entorno digital. Como padres, madres, maestros, maestras, profesoras, profesores o educadoras y educadores, debemos ser un ejemplo y transmitir a los menores la importancia de la privacidad y que tienen que tener cuidado con quién comparten información en la Red.

2.2. LOPD y RGPD

¿Qué es la LOPD?

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) es la ley con carácter doméstico que se encarga de la transposición de la Directiva 95/46/CE que hasta el 25 de mayo de 2016 ha sido el texto de referencia, a escala europea, en materia de protección de datos personales.

En concreto la Directiva creó un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE), fijando límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales.

¿Qué es el RGPD?

El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD), que será de aplicación el próximo 25 de mayo de 2018. A diferencia de lo que ocurrió con la Directiva 95/46/CE, la naturaleza del Reglamento es que es de aplicación directa y por tanto no necesita ninguna ley de carácter nacional para implementarlo, simplemente que la ley que se encargue de regular este aspecto, en este caso la protección de datos, contemple las previsiones ya establecidas en el Reglamento.

Por este motivo, a partir del 25 de mayo de 2018 entra en vigor la nueva Ley Orgánica de Protección de Datos de Carácter Personal, de la cual ya salió un Proyecto de Ley el 24 de noviembre de 2017.

El 25 de mayo de 2018 comenzará a ser de aplicación el Reglamento General de Protección de Datos (RGPD) a todas las empresas que operan en la Unión Europea, sustituyendo la Ley Orgánica de Protección de Datos del año 1999.

Vamos a ver a qué cambios tienen que enfrentarse las empresas para cumplir con la nueva reglamentación y cómo se diferencia de lo ya establecido por la LOPD actual.

LOPD vs. RGPD

Si bien muchos de los conceptos y principios del RGPD son parecidos a la norma actual, el RGPD introduce nuevos elementos, que suponen nuevas obligaciones para las empresas y organizaciones de la UE.

Conforme nos vamos acercando a la fecha límite, el cumplimiento con las nuevas normas se hace necesario, no solo por una de las principales novedades que son las sanciones de hasta un 4% de la facturación global anual o 20 millones de euros que se establecen, sino por la relevancia de que para muchos negocios de publicidad digital, por vez primera será necesario cumplir con las normas de protección de datos.

Tabla resumen de novedades		
Obligaciones para la empresa	**Derechos para los usuarios.**	**Nueva figura**
• Proactividad • Evaluación de Impacto sobre la Protección de Datos (EIPD)	1. Consentimiento libre, específico, informado e inequívoco. 2. Derecho de acceso 3. Derecho al olvido. 4. Solicitar que cesen las operaciones de tratamiento de sus datos. 5. Portabilidad.	Delegado de Protección de Datos (DPD).

- **Obligaciones para la empresa**

  El primer paso que todas las empresas deberían ejecutar es identificar y analizar las áreas de riesgo y documentar los tratamientos de datos personales que se llevan a cabo, a través de un inventario de todas las actividades de tratamiento que realiza la compañía. Este enfoque exige una **proactividad** por parte de cada organización para analizar estos aspectos, determinar los riesgos y en función de su nivel, establecer las medidas necesarias para minimizarlo.

  En los casos en los que se detecten tratamientos con un alto riesgo cara a los derechos y libertades de los interesados, deberá realizarse adicionalmente una **Evaluación de Impacto sobre la Protección de Datos (EIPD)** e introducir las

medidas necesarias para la mitigación de los mismos.

Esta obligación también se extiende a lo que conocemos como brechas de seguridad, que pueden tener importantes consecuencias, por lo tanto, las empresas deben asegurarse de poner en marcha todos los procedimientos que permitan detectar, informar e investigar una brecha de seguridad.

- **Derechos para los usuarios.**

  El RGPD amplía los derechos con la limitación de tratamiento a los datos indispensables para prestar un servicio y una vez acabado tendrán que dejar de utilizarlos, pero también regula una serie de derechos adicionales a los tradicionales ARCO, de tal forma que los usuarios tendrán:

  1. **Consentimiento libre, específico, informado e inequívoco**. No se aceptará el consentimiento tácito o por omisión;
  2. **Derecho de acceso:** Se puede ahora obtener una copia de los datos personales que se estén tratando.
  3. **Derecho al olvido**.
  4. Los interesados pueden **solicitar que cesen las operaciones de tratamiento** de sus datos.
  5. **Portabilidad**. Los interesados podrán recibir los datos personales que han proporcionado a un responsable del tratamiento, en un formato estructurado, de uso común y legible.

- Finalmente, el Reglamento introduce una figura nueva que es el **Delegado de Protección de Datos (DPD)**. El RGPD estipula que uno de los criterios para decidir si es necesario designar un delegado de protección de datos es cuando las actividades principales del responsable o del encargado requieran una “observación habitual y sistemática de interesados a gran escala”.

El DPD puede ser, sin ir más lejos, un trabajador de la entidad o un consultor externo, encargado de comprobar y registrar el tratamiento que se realiza de los datos personales dentro de la organización.

3. ¿Qué es la identidad digital?

Gaia nació por la noche y sus primeras fotos estuvieron en las redes sociales una hora después del festejo, la alegría y regocijo de sus padres y familiares. Esa fotografía (la de una niña recién nacida envuelta en la cobija del hospital) no era la primera que conocía el mundo.

A los tres meses de gestación un ecógrafo captó la primera imagen de Gaia en el vientre materno, cuando aún era un pequeño bulto que recién comenzaba a tener forma humana. Luego vinieron las imágenes en sepia del mismo aparato, los videos en tercera dimensión, a color y en los que se escucha el ritmo de los latidos de su corazón, todo se subió a la red.

La pequeña ya tenía nombre antes de nacer, gracias al aparato de ultrasonido, que confirmó su sexo en la semana veinte del embarazo de su madre. Sus padres decidieron bautizarla Gaia, como la diosa de la tierra. La tierna Gaia recibió comentarios en el muro de Facebook de su padre, sin saber leerlos; recibió likes, sin entenderlos; su foto fue compartida, sin pedirlo, entre familiares y amigos vía Twitter, Facebook, WhatsApp o por el e-mail que mandó su padre al día siguiente.

A la inocente Gaia las imágenes ya la rebasaron y aún no tiene un día de vida. Acaba de nacer Gaia, una nativa digital. Su presencia virtual fue previa a su presencia real en este mundo.

Cada vez el mundo virtual parece obtener mayor protagonismo y legitimidad que el mundo real. Cada día, miles de personas se comprometen, consciente o inconscientemente, a que su imagen esté presente y vigente en las redes sociales actualizando fotos, estados de ánimo, o adhiriendo gente como “amigos”, cuando jamás llegarán a conocerlos personalmente. Debido a esa característica, aceptada involuntariamente por los mismos usuarios, las redes sociales como Facebook configuran sus herramientas para que todo sea más público y todo menos privado. Cada vez más usuarios se conectan a esta dinámica, mientras son estigmatizados los que desean vivir fuera o alejados del mundo virtual. Facebook rebasó los 2.197 millones de usuarios y más de 70 idiomas; en Ecuador, en el año 2018, de enero a julio.

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)

Al inicio del capítulo hemos visto un ejemplo de cómo **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.

A continuación vamos a ver algunos conceptos ligados a identidad digital.

3.1. ¿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.**

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.

El rastro que conforma la identidad digital está formado por una serie de impactos de distinta procedencia, algunos son:

- **Perfiles personales:** Redes sociales (como lo son Facebook, twitter y profesionales (como Xing, LinkedIn) y portales de búsqueda de empleo.
- **Comentarios**: En foros, blogs, portales de información, redes sociales y YouTube.
- **Contenidos digitales:** Fotos en redes sociales, videos en vimeo, presentaciones en onslideshare o documentos publicados en webs, una web personal , un blog.
- **Contactos**: Puede ser nuestros amigos, contactos personales, seguidores, a quienes seguimos y correo electrónico.
- **Mensajería instantánea:** Como por ejemplo, Whatsapp.

Es muy sencillo subir fotografías, vídeos o comentarios a Internet, pero no es tan fácil borrarlos. En Internet, las huellas que dejamos, son difíciles de borrar.

Por todo ello, debemos trasladar a los menores que:

- Es muy importante que seamos selectivos a la hora de publicar cualquier tipo de información en Internet. Tengamos en cuenta que la foto más graciosa o traviesa o el comentario más perspicaz puede no serlo dentro de unos años.
- Es fundamental explicarles la importancia de esta huella digital así como la perdurabilidad de la información en Internet.

3.2. ¿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.

La reputación online es el reflejo del prestigio o estima de una persona en Internet:

- **Importancia de la reputación online en la adolescencia.** Para los adolescentes tiene mucha importancia la reputación que tienen en la red, ya que quieren ser "populares". Por ello, suelen subir contenidos buscando siempre la aceptación y aprobación de sus compañeros/as e iguales.
- **Falta de controlabilidad de esta reputación.** La reputación online solo es controlable por el adolescente de forma parcial, ya que se genera en gran medida por las opiniones y comentarios que vierten los demás sobre él/ella.
- **Posibles consecuencias.** El adolescente corre el riesgo de entrar en una "guerra" para incrementar su popularidad en la red, subiendo cada vez contenidos más íntimos y privados a la red.

Como podemos ver, la gestión de la privacidad conforma la huella digital que se deja en la red, que a su vez, da forma a nuestra identidad digital. Esta identidad, observada por los demás, genera nuestra reputación online. Estos conceptos son piezas de un engranaje al que hay que cuidar en su totalidad.

4. Otros factores que afectan a la privacidad

4.1. Publicidad, consumo y privacidad

Detrás de la inmensa mayoría de servicios existe un negocio basado en el negocio de los datos que suben los usuarios a la red. La publicidad es clave en el ámbito online y en los últimos años se ha especializado en el análisis del comportamiento de los usuarios, a través de las **cookies** del navegador o con los identificadores únicos de los smartphones.

Las **cookies** están especialmente diseñadas para facilitar la navegación del usuario que accede a un servicio por Internet. Para facilitar esto recoge información que se puede utilizar para ofrecer una publicidad basada en sus hábitos de navegación. Esta estrategia muestra anuncios basándose en la localización del usuario o en páginas web que el usuario ha visitado recientemente.

¿Cómo funcionan? Utilizar **cookies** supone la descarga de un archivo o dispositivo en el equipo con la finalidad de almacenar y recuperar datos que se encuentran en el citado equipo. Esto tiene implicaciones importantes en relación con la privacidad ya que esa información es importante a la hora de ofrecer una publicidad adaptada a nuestros intereses.

Por ello 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.

La publicidad en Internet expone de forma diferente a los menores a la publicidad que se realiza desde la televisión u otros medios de comunicación debido a su interactividad y a la mayor inmersión de éstos en Internet. Vamos a 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.
- **Publicidad a través de móvil**: Este tipo de publicidad a crecido exponencialmente por el elevado uso de los smartphones entre la población joven. Todas las técnicas que hemos mencionado anteriormente pueden utilizarse igualmente teniendo en cuenta que cuando nos descargamos una aplicación determinada y aceptamos los permisos que necesita, la compañía que la gestiona en muchas ocasiones puede acceder a información sobre nosotros que puede utilizar para enviarnos publicidad.

4.2. Privacidad en las APPS (Aplicaciones móviles)

El uso de aplicaciones para dispositivos móviles como el resto de servicio en Internet pueden plantear importantes riesgos para la vida privada de los usuarios si no cumplen la legislación sobre protección de datos vigente en la actualidad.

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. Por ello los desarrolladores de aplicaciones:

- Deben informar tanto sobre los datos a recopilar como sobre los usos y finalidades de los mismos.
- Es 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.

Cuando se utilizan aplicaciones móviles se requiere un registro previo por parte del usuario o dar permisos para acceder a información ubicada en el teléfono. Hemos de tener en cuenta que en dicho uso se están facilitando datos personales que pueden suponer riesgos para la seguridad.

Uno de los riesgos a destacar es la geolocalización que permite a partir de la localización física del mundo real ofrecer una serie de servicios. Estas aplicaciones suelen hacer uso de la geolocalización para:

- 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 (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 como Google Maps.

- 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.

La mayoría 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. 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) con el objetivo de fomentar el cumplimiento de la legislación de protección de datos y privacidad, promover la concienciación de los usuarios y obtener una visión integral y conjunta.

4.3. Protección de la privacidad de terceros

Además de prestar atención a la buena gestión de la propia privacidad, hemos de ser conscientes de respetar esta privacidad de terceras personas con nuestro comportamiento.

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 debemos pensar siempre antes de publicar una información que no sólo nos pertenece a cada uno, tal como fotos o videos en los que aparezcan otras personas.

Aunque 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 consentimiento.

5. Los menores en la red

Supongo a que estas alturas del curso nos surge una preguntas ¿porqué los menores suelen exponerse tanto en Internet?

La notoriedad o popularidad, reconocimiento, aprobación, aceptación, autoafirmación, buscar nuevas experiencias o encontrar a gente con aficiones en común son respuestas que encontramos ante las diferentes situaciones que pueden producirse.

A continuación vamos a ver algunas de las motivaciones que les lleva a actuar como lo hacen.

5.1. Motivaciones de los menores para su exposición en Internet

Una de las razones a destacar por la que los menores se **sobreexponen** 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 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.

5.2. 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.1
  - **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.

6. Datos de situación

Estudios sobre la privacidad de los menores en Internet

La sección española del proyecto EU Kids online ha dado a conocer los resultados y según sus datos:

- Sólo el 55% de los menores sabe cómo cambiar su configuración de privacidad en las redes sociales. Además hay un gran número de menores que las están usando por debajo de la edad permitida legalmente.
- 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…).

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.

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.

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.

- 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 años17:
  - 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.

- 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 países18. Además, resulta interesante destacar que:
  - Los niños más pequeños son más propensos que los mayores a tener su perfil "público".

- 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).

6.1. La privacidad en el futuro

¿Cuál es el futuro de la privacidad? Que lo marquen las compañías que viven de su explotación, claramente, no parece el mejor de los escenarios. Pero que lo hagan los gobiernos, interesados en mayor o menor medida en el control de su población, tampoco parece asegurar un futuro mínimamente garantista.

Posiblemente, la mejor baza esté en la acción ciudadana, basada en un nivel de información lo más riguroso posible: mientras una parte importante de la población siga sin darle importancia al tema, sin preocuparse de conocer o controlar las opciones de privacidad de los productos que utilizan, o pensando que “como no tienen nada que ocultar, no tienen nada que temer“, la solución al problema seguirá estando lejos.

Que muchos usuarios se manifiesten cada vez más molestos por los niveles de agresividad e intrusión de la publicidad en la red sí que es importante, porque es una posición más activa, pero tampoco garantiza nada, y de hecho, parece estar desembocando en una situación en la que conseguir un nivel adecuado de protección de la privacidad solo está al alcance de “los más listos”, de aquellos que saben buscar el conjunto de herramientas suficiente para hacer frente a la situación.

La administración **Trump** publicó el mes pasado una propuesta, que probablemente dará forma a la futura legislación que pueda venir en este sentido, en la que aboga por **dar a los usuarios más controles sobre la forma en la que sus datos son utilizados por las compañías tecnológicas**. La propuesta tiene sentido viniendo de quien viene, el

presidente que más bombardea a sus ciudadanos a través de las redes sociales con publicidad microsegmentada, que se beneficia precisamente del hecho de que una compañía ofrezca supuestamente a sus usuarios todas las opciones posibles para tomar decisiones sobre el nivel de privacidad que desean, pero que, a pesar de los sucesivos problemas que experimenta en ese sentido, consigue que sean pocos los que entren a cambiar esas opciones. El caso de **Facebook**, que parece empeñada en demostrar que si puede acceder y explotar cualquier tipo de dato personal de sus usuarios lo hará con total seguridad, es paradigmático: si hace algunos días hablábamos la presentación de su nuevo dispositivo enfocado a videoconferencias, Facebook Portal, y de las garantías de la compañía de no utilizarlo para captar datos, ahora la compañía se desdice y clarifica que aunque el dispositivo no mostrará publicidad, los datos que pueda captar sobre sus patrones de uso sí podrán ser utilizados para segmentar la publicidad en otras propiedades de la compañía.

Al tiempo, **Google** nombra a un nuevo responsable de privacidad y marca los que considera sus criterios para una posible regulación federal del tema, igualmente centradas en ofrecer más poder al usuario para decidir sobre los niveles de privacidad que desea. El problema, sin duda, es complejo: si bien mucho podrían pensar, de manera intuitiva, que si les permiten decidir sobre el nivel de privacidad que desean tenderían a escoger los niveles más garantistas y cerrados, la realidad es que la gran mayoría de los usuarios simplemente no se preocupan del tema o prefieren conscientemente permitir que el estudio de sus patrones de uso sean utilizados para mejorar la propuesta de valor de los productos y servicios que utilizan.

La Unión Europea, por otro lado, a pesar de que ha cometido errores clamorosos que han creado muchos más problemas de los que soluciona, inventándose derechos artificiales e inexistentes que no hacen más que provocar problemas e incoherencias en sus intentos de aplicación, mantiene una línea de defensa de los usuarios, plasmada en el desarrollo del reglamento general de protección de datos (GDPR), que podría significar un paso interesante, si prueba tener el adecuado poder sancionador, a la hora de corregir abusos y usos malintencionados por parte de las compañías.

En otros entornos, como el caso tantas veces comentado de **China, todo indica que la batalla está claramente perdida**: la privacidad es una variable bajo un dominio omnímodo del estado, capaz de agregar cualquier dato obtenido por cualquiera de los actores de la industria, y que la utiliza sin ningún tipo de problema para el control social – a pesar de algunos tímidos episodios de resistencia en ese sentido – en un entorno en el que la mayoría de los ciudadanos, simplemente, carecen ya prácticamente de cualquier expectativa de privacidad y lo ven como algo que no les importa excesivamente. Por otro lado, ni siquiera está claro cuáles de los países que consideramos supuestamente democráticos tienen un genuino interés en preservar la privacidad de sus ciudadanos como un derecho fundamental o cuáles, en realidad, envidian secretamente el nivel de control que ejerce el gobierno chino.

¿Empresas? ¿Gobiernos? ¿Usuarios? ¿Quién y cómo debería condicionar la agenda en la evolución futura de un concepto como la privacidad?

7. Bibliografía

- Dans E (2018), ¿Quién debe marcar el futuro de la privacidad? Recuperado de: https://www.enriquedans.com/2018/10/quien-debe-marcar-el-futuro-de-la-privacidad.html
- Digital in 2018: Q3 Global Digital Statshot. Recuperado de: https://es.slideshare.net/wearesocialsg/digital-in-2018-q3-global-digital-statshot
- Instituto Nacional de Tecnologías de la Información INTECO. (2012). Guía para usuarios: identidad digital y reputación online. Recuperado de: https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/guia_identidad_digital
- Monográfico gestión de la privacidad e identidad digital. Recuperado de: http://bullying-acoso.com/wp-content/uploads/2018/02/Monografico-Gestion-de-la-privacidad-e-identidad-digital_Red.es_-1.pdf
- Pantallas Amigas. Recuperado de: http://www.pantallasamigas.net
- Portal del menor. http://www.portaldelmenor.es
- Privacidad online. Recuperado de: http://www.privacidad-online.net
- Real Academia Española. (2001). Privacidad. En Diccionario de la lengua española (22.a ed.). Recuperado de http://lema.rae.es/drae/?val=privacidad
- RGPD y LOPD: ¿Qué diferencia hay?. Recuperado de: https://letslaw.es/diferencia-rgpd-lopd/
- Yo virtual, yo real. Recuperado de: https://www.eltelegrafo.com.ec/noticias/carton/1/yo-virtual-yo-real