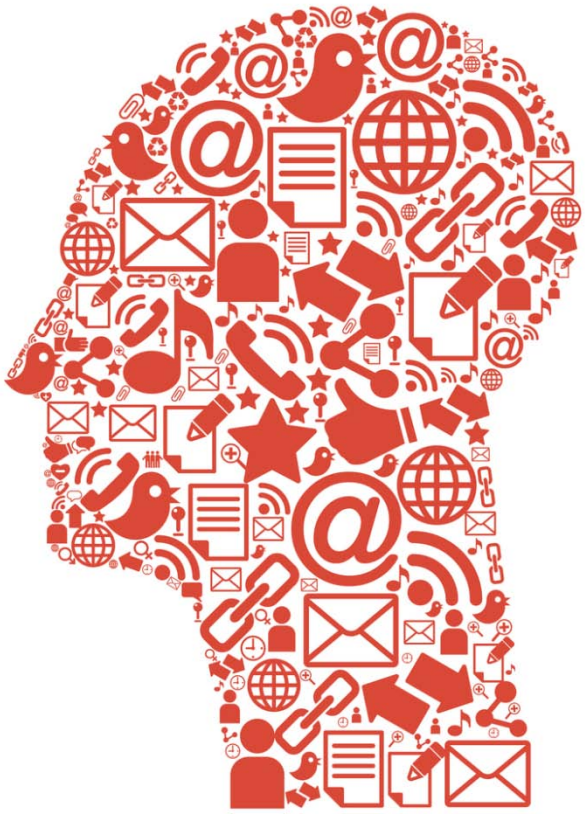
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía para usuarios:
identidad digital y reputación online



INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN

Edición: Julio 2012

La “Guía para usuarios: identidad digital y reputación online” ha sido elaborada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO:

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Susana de la Fuente Rodríguez (coordinación)

Eduardo Álvarez Alonso

Laura García Pérez

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las administraciones y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en España, promoviendo además una línea de participación internacional. Para ello, INTECO desarrolla actuaciones en las líneas de Seguridad, Accesibilidad, Calidad TIC y Formación. Más información: http://observatorio.inteco.es

En la elaboración de esta guía, INTECO ha contado con el apoyo técnico de:

Índice

1. Introducción

El desarrollo de las Tecnologías de la Información y la Comunicación, y en especial Internet, ha creado un nuevo escenario en el que las relaciones personales cobran protagonismo. Los servicios de Internet y la Web 2.0 (redes sociales, blogs, foros, wikis, *microblogging*, etc.) constituyen canales multidireccionales y abiertos, que permiten a sus usuarios lograr la máxima interacción entre ellos, a la vez que ofrecen nuevas posibilidades de colaboración, expresión y participación. En este contexto, indudablemente, el ciudadano se muestra con una serie de atributos que definen su personalidad online.

Las TIC consiguen crear una "identidad expandida" en la mayoría de sus usuarios: potencian sus habilidades y les permiten estar en contacto con otros usuarios manteniendo diferentes niveles de relación, intimidad, compromiso, etc.

Una gran parte de los internautas ya están desarrollando esas capacidades y utilizando las ventajas que engloba la idea de identidad digital con diferentes grados de compromiso, adscripción o revelación de su privacidad[1].

> *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.*

La reputación es una construcción social, un producto creado y acumulado de forma colectiva y que de manera inevitable tiene efectos positivos o negativos al tener una connotación pública. Igualmente queda patente que al tratarse de una construcción alrededor de las percepciones de otros, nuestra reputación no está bajo control de manera absoluta, ni siempre ni por completo, aunque sí se puede gestionar en la medida en que se construyan de manera adecuada esas percepciones a partir de hechos relevantes para la opinión individual y colectiva.

> *La **reputación online** es la opinión o consideración social que otros usuarios tienen de la vivencia online de una persona o de una organización.*

Identidad digital y reputación online, pues, son dos conceptos estrechamente relacionados. La identidad es lo que yo soy, o pretendo ser, o creo que soy. La reputación, mientras, es la opinión que otros tienen de mí[2].

---

[1] VARELA, J. "La forja de una identidad digital". Red.es, disponible en: http://www.red.es/reportajes/articles/id/3545/forja-una-identidad-digital-.html

[2] ALONSO, J. "Identidad y reputación digital". Evoca. Cuadernos de comunicación, disponible en: http://www.evocaimagen.com/cuadernos/cuadernos5.pdf .

Precisamente, en la exposición de nuestra identidad en Internet nos enfrentamos a desafíos que pueden constituir amenazas a nuestra privacidad y seguridad. ¿Qué ocurre cuando alguien es víctima de suplantación de identidad?, ¿o cuando se publican fotografías nuestras que no deseamos que estén disponibles en Internet?

Esta guía tiene como objetivo proporcionar al lector pautas que le ayuden en la construcción de su personalidad en el entorno virtual. Es responsabilidad de cada uno, como miembros de esta comunidad de internautas, gestionar de manera responsable nuestra identidad digital y reputación online.

El objetivo general de la guía es desarrollar un análisis riguroso de los conceptos de identidad digital y reputación online de las personas, desde el punto de vista de la privacidad y seguridad, generando conocimiento en cuanto a los riesgos existentes y aportando una serie de pautas de actuación y recomendaciones para la gestión de la identidad y reputación online.

Con este objetivo, la presente guía abarca los siguientes apartados:

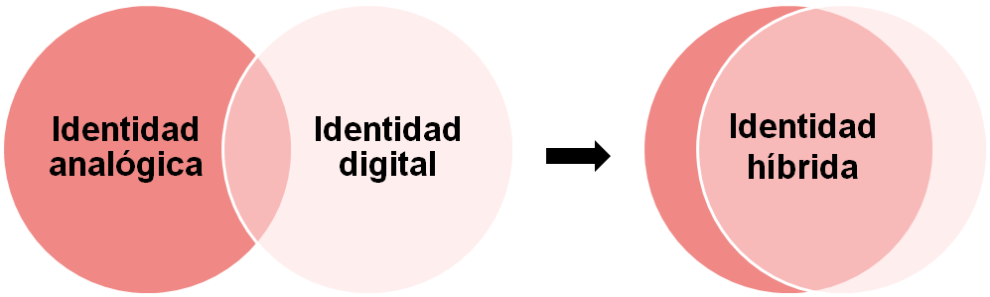
- La identidad digital.
- La reputación online.
- Riesgos en la gestión de la identidad digital y reputación.
- Marco legal.
- Recomendaciones para la gestión de la identidad digital.
- Buenas prácticas en la gestión de la identidad digital.
- Bibliografía.

2. La identidad digital

La identidad en el entorno físico, o identidad analógica, se ha venido basando tradicionalmente en la asignación e inscripción registral de unos determinados datos y su acreditación mediante documentos físicos seguros, con carácter oficial y exclusivo.

La identidad digital es, en contraste, un concepto muy amplio, enfocado en la vivencia de los ciudadanos en la Red, que incluye las funciones de la identidad analógica, y las supera, debido a las nuevas posibilidades que ofrece.

De forma progresiva, la identidad analógica y la identidad digital forman parte de una misma realidad, en la que no se distingue entre la actuación realizada en el mundo físico y en la Red, de forma que se puede hablar de convergencia hacia la identidad híbrida.



Convergencia hacia la identidad híbrida

Sin embargo, es posible que la construcción de la identidad digital no esté expresamente ligada al "yo" analógico de la vida *real*. Sería el caso de personalidades online totalmente ficticias creadas a partir de datos inventados por el usuario.

2.1 PROPIEDADES

La identidad digital presenta una serie de propiedades, identificadas por la OCDE[3]:

- **La identidad digital es esencialmente social.** A medida que el individuo proyecta su personalidad en la Red, especialmente en las redes sociales, sus vecinos digitales le caracterizan y reconocen de forma efectiva, incluso en ocasiones en que no se ha producido una verificación presencial de la identidad.

- **La identidad digital es subjetiva.** Tanto la percepción del "yo" como del "nosotros" están basadas en la experiencia que personas diferentes construyen y que les permiten reconocerse.

[3] RUNDLE, M.; TREVITHICK, P. *At a crossroads: 'Personhood' and digital identity in the information society*, STI Working Paper 2007/7. Directorate for Science, Technology and Industry. OECD, 2008.

- **La identidad digital es valiosa.** La propia actividad de los sujetos genera capital informacional que puede ser empleado para establecer relaciones personalizadas y para tomar decisiones en las relaciones con las personas, con un mayor grado de confianza.

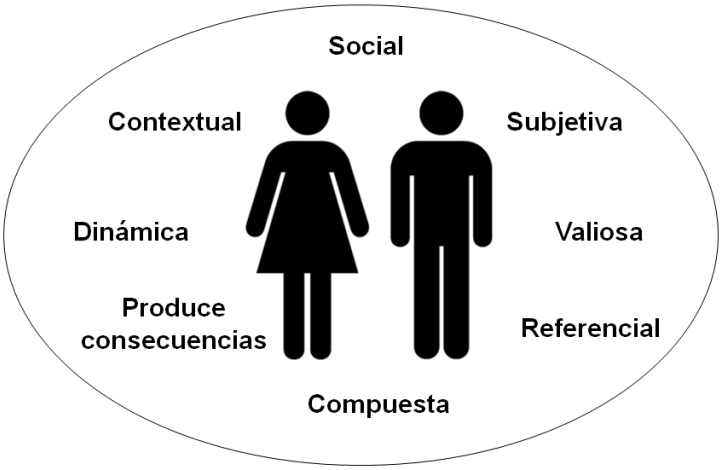
- **La identidad digital es referencial.** De hecho, una identidad no es una persona o un objeto, sino una referencia a dicha persona u objeto.

- **La identidad digital es compuesta.** Mientras que algunas informaciones son suministradas de forma voluntaria por los propios usuarios, otras informaciones sobre los mismos son construidas por terceros, sin la participación del sujeto en cuestión.

- **La identidad digital produce consecuencias.** La divulgación de la información en ocasiones puede generar efectos, y en otros casos, es la no divulgación la que constituye una amenaza por sí misma.

- **La identidad es dinámica**, porque se encuentra en cambio y modificación permanente. Especialmente en Internet, la identidad digital se debe ver como un flujo de informaciones, en lugar de como una foto fija de una persona.

- **La identidad es contextual.** Dado que la divulgación de la información puede generar un impacto negativo empleada en un contexto erróneo, o sencillamente ser irrelevante, mantener las identidades segregadas entre sí permite tener más autonomía.



Propiedades de la identidad digital (OCDE)

2.2 IDENTIDAD DIGITAL: ¿ÚNICA O MÚLTIPLE?

Los elementos que integran la identidad digital y que permiten a las personas físicas diferenciarse frente a otras en ámbitos concretos son los rasgos de identidad o atributos informativos: nombre y apellidos, correo electrónico, datos de contacto, fotografías, vídeos, información laboral, aficiones, preferencias políticas, religiosas o sexuales, dirección IP, datos de geolocalización y un largo etcétera.

En definitiva, es un rasgo de identidad cualquier pieza de información personal que forme parte del puzle de la identidad online.

Los rasgos de identidad se suelen encontrar agrupados o relacionados entre ellos, formando **identidades parciales**. Las personas físicas utilizan diferentes identidades parciales en función de los diferentes roles y actividades que desarrollan a lo largo de su existencia online. Cada identidad parcial está sustentada en un servicio o aplicación de Internet. Así, por ejemplo, un usuario mantiene sus perfiles en Facebook, Twitter y Linkedin, participa con el mismo alias en distintos foros de profesionales, gestiona un blog de viajes y aparece ocasionalmente en prensa y webs especializadas, relacionadas con su ámbito profesional.

Todo ello conforma la identidad digital del sujeto, pero cada uno de los servicios mencionados sustenta una identidad parcial, que puede aparecer relacionada (o no) con el resto.

La vivencia online, esto es, la suma de las diferentes identidades parciales, permite construir una identidad digital: una imagen de la persona en Internet.

3. La reputación online

La reputación es la opinión o consideración en que se tiene a alguien o algo, o el prestigio o estima en que son tenidos alguien o algo. El individuo que desarrolla su actividad aspira a ser percibido positivamente por su entorno y, por tanto, a poseer una buena reputación. Por ello, como más adelante se examina, el Derecho provee de acciones en aquellos casos en los que, sin justificación alguna, ésta se lesiona. En este contexto, el concepto de reputación es perfectamente trasladable a Internet.

Internet ha introducido cambios cualitativos particularmente significativos, no tanto en el concepto de reputación, como en el modo de construirla, mantenerla y defenderla. Veamos a continuación de qué forma y cuáles son las diferencias:

- En primer lugar, la reputación online no es tanto lineal sino **acumulativa** en el tiempo. Así, en el contexto pre-Internet, la reputación se construía de manera lineal a lo largo del tiempo. De esta manera, la reputación lo era en un momento histórico concreto, pudiendo haber ganado (o perdido) solidez a lo largo de un período temporal.

  El concepto de reputación en el mundo de Internet no facilita esta visión lineal de la historia de un individuo. La Red no permite el olvido de manera sencilla, ya que cada acción en Internet deja trazas. Así, en la reputación de un sujeto medida en el momento actual influirán sus acciones, positivas y negativas, llevadas a cabo en cualquier momento pasado.

  A un click de distancia se encuentra información personal que dibuja las vivencias de la persona. No es difícil averiguar, por ejemplo, que en su adolescencia ha resultado ganador/a de una olimpiada matemática, o que entre sus hobbies se encuentra el ajedrez y las carreras populares, o la empresa en la que presta sus servicios. También están fácilmente localizables en la Red informaciones sobre impagos o multas, que quizás no sean del agrado del usuario en cuestión.

  En definitiva, la reputación en Internet se forma a partir de una enorme cantidad de información personal, con independencia del momento en el que fue generada. Cada acción en Internet deja trazas que pueden ser localizadas y tratadas de modo independiente y ajeno a la voluntad de la persona, y de forma asíncrona, ya que la Red no permite fácilmente el olvido asociado al transcurso del tiempo.

- La segunda diferencia tiene que ver con la **repercusión y el alcance de la reputación personal**. En la era pre-Internet, la difusión de las acciones de un ciudadano anónimo tenía un alcance limitado al ámbito más cercano, familiar, profesional y social.

No ocurre así en el entorno online. Cualquier persona posee la capacidad de lanzar información y opiniones en el mundo 2.0, que a su vez es susceptible de ser localizada, indexada, copiada y enlazada, alcanzando una elevada difusión. Todos tenemos una reputación online, en mayor o menor medida. Es conocida la máxima que reza, precisamente, "si no estás en Google, no existes".

3.1 FACTORES DETERMINANTES DE LA REPUTACIÓN ONLINE

La construcción de la reputación digital de una persona física depende de múltiples factores. Entre ellos, resulta determinante la presencia o no de un objetivo claro por parte del propio sujeto. Pueden apuntarse al menos tres factores determinantes en la caracterización de la reputación online:

1) **Las acciones emprendidas por el propio sujeto.** Evidentemente, se trata del primer elemento a considerar en la construcción de la reputación online: el modo en el que una persona se muestra, trasladando a entornos 2.0 aspectos pertenecientes a su vivencia particular, alimenta y enriquece su biografía, y es un elemento importante que determina cómo le ven los demás. Cualquier acción que emprendemos en la Red deja un rastro que forma parte, inevitablemente, de cómo nos perciben los demás.

   En este sentido, se ha desarrollado un nuevo concepto: "extimidad", que viene a significar "hacer externa la intimidad". Hace alusión a aquéllos que, de modo habitual, trasladan al contexto de la red social el conjunto de acontecimientos vitales que les incumben, redactando así una autobiografía en tiempo real.

2) **Información generada por otros y accesible a través de servicios disponibles en Internet**, como buscadores o servicios de publicidad altamente personalizada. Se trata de contenidos publicados por parte de terceras personas, por ejemplo, periódicos y otros medios de comunicación, artículos de opinión, boletines, etc., que, por su relevancia pública, han podido trascender. En realidad, deben distinguirse dos impactos distintos: el contenido mismo de la información (que tendrá un efecto positivo o negativo sobre la reputación), y el posicionamiento en los buscadores (no es lo mismo aparecer entre los primeros diez resultados que en páginas secundarias). Puede ocurrir que el resultado ofrecido por el buscador sitúe en mejor posición una determinada información perjudicial sin ofrecer, por ejemplo, ningún registro complementario que aclare aquella.

   Es importante ser conscientes de la posibilidad más real que potencial de que terceros generen registros biográficos de una persona (*lifelogs*), a partir de la información disponible en múltiples entornos de Internet y, en particular, en las aplicaciones de redes sociales.

3) **Las acciones emprendidas en el ámbito relacional del sujeto.** Del mismo modo que en el mundo físico las buenas o malas relaciones personales afectan a la reputación personal, en el mundo online un comentario o actitud inadecuados definen la imagen que se muestra a los demás. Pero además, permanecen en el tiempo y pueden difundirse sin límites.

El número de seguidores que tenemos, sus reacciones y comentarios a nuestras acciones, son el tercer factor a tener en cuenta en la construcción de nuestra reputación online.

Una correcta gestión de nuestra reputación online implica actuar sobre tres elementos: el contenido generado por nosotros mismos, el contenido sobre nosotros generado por terceros y el contenido generado en el marco de las relaciones con los demás.

A continuación se profundiza en qué papel juega el individuo en la construcción de su reputación online.

3.2 EL PAPEL DEL INDIVIDUO EN LA CONSTRUCCIÓN DE SU REPUTACIÓN ONLINE

Puede afirmarse que aprender a interactuar con terceros y manejar aspectos básicos de *personal branding* o construcción de una marca personal puede convertirse en algo esencial para el desarrollo de la personalidad y el futuro social y profesional.

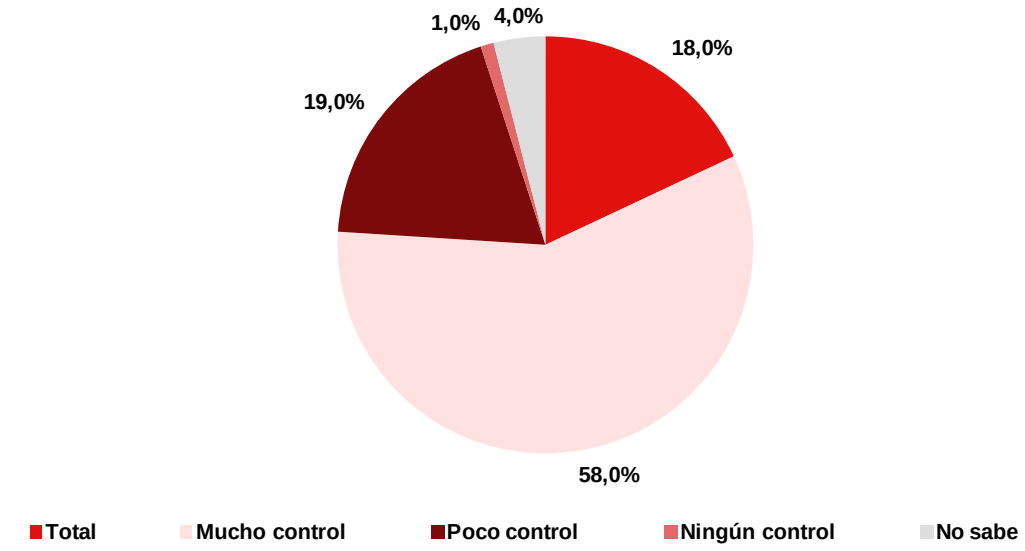
Dedicar esfuerzo a construir tu propia identidad digital ya no es opcional. Es un acto de pura responsabilidad

3.2.1 Percepción de control sobre la reputación online propia

Parece evidente que la capacidad de control sobre los tres factores determinantes de la reputación online del individuo (contenido generado por el propio individuo, contenido generado por terceros y contenido generado en el contexto relacional del sujeto) es diferente en cada uno de los casos. A priori, se podría pensar que el control que un usuario cree tener sobre contenidos publicados por un tercero que afectan a su reputación es limitado.

Sin embargo, la mayoría de los internautas tienen una percepción de control sobre su reputación online. Así, según los datos proporcionados por Microsoft para el mercado español (basado en una encuesta a 500 adultos usuarios de Internet de entre 18 y 74 años), el 18% de los sujetos consideraría que tiene un control total sobre su reputación online, y un 58% adicional pensaría que ejerce mucho control.

Gráfico 1 Percepción de control que tiene el usuario de Internet español sobre su reputación online



n=500 **Fuente: Microsoft (2012)**

3.2.2 Configuración de privacidad del perfil en redes sociales

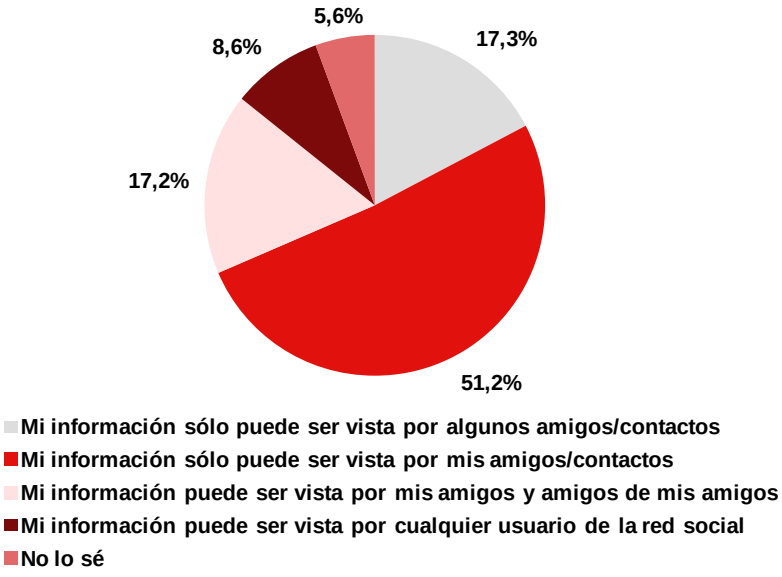
La reputación online de los individuos se encuentra conectada la dignidad personal y el control de la imagen personal. Por este motivo, la reputación online se relaciona directamente con la posibilidad de controlar la visibilidad de las propias vivencias digitales, de forma que, en su caso, sólo las personas autorizadas puedan acceder a las mismas.

Una de las fórmulas más sencillas para controlar la reputación en línea es la gestión adecuada de la visibilidad de los perfiles en redes sociales. Se trata de un primer paso, necesario, en la construcción de una identidad digital coherente con lo que el usuario desea comunicar sobre sí mismo.

En general, los internautas españoles son prudentes a la hora de decidir quién puede acceder a la información que publican en redes sociales[4].

Según los resultados de la encuesta realizada por INTECO, más de la mitad de los usuarios de redes sociales restringen la visibilidad de su información exclusivamente a su círculo de amigos, mientras que un 17,2% permite el acceso a amigos y amigos de sus amigos. Solo un 8,6% reconoce que su perfil está accesible a cualquier usuario de la red social, lo que puede constituir una práctica poco prudente.

Gráfico 2: Nivel de privacidad del perfil del usuario de redes sociales en 3er cuatrimestre 2011 (%)



Base: Usuarios de redes sociales (n=3.294) **Fuente: INTECO**

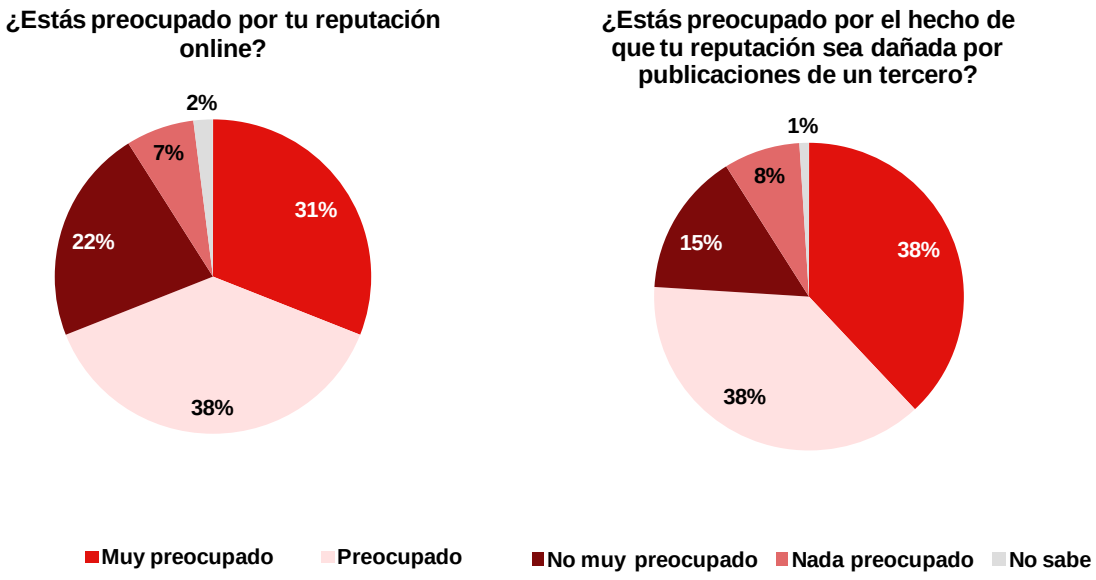
[4] Fuente: Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles, 3er cuatrimestre de 2011. INTECO (2012).

3.2.3 Preocupación por la reputación online

Los usuarios se sienten más preocupados por su reputación online precisamente cuando son terceros los que publican o difunden informaciones que les conciernen.

Esta afirmación puede extraerse del hecho de que el 31% de los usuarios de Internet españoles de entre 18 y 74 años se muestre muy preocupado por su reputación online, en general. Más aún, el porcentaje alcanza el 38% cuando se trata de determinar el nivel de preocupación por efecto de publicaciones de terceras personas sobre su reputación online.

Gráfico 3 Preocupación de los internautas españoles (18-74 años) por su reputación online (%)



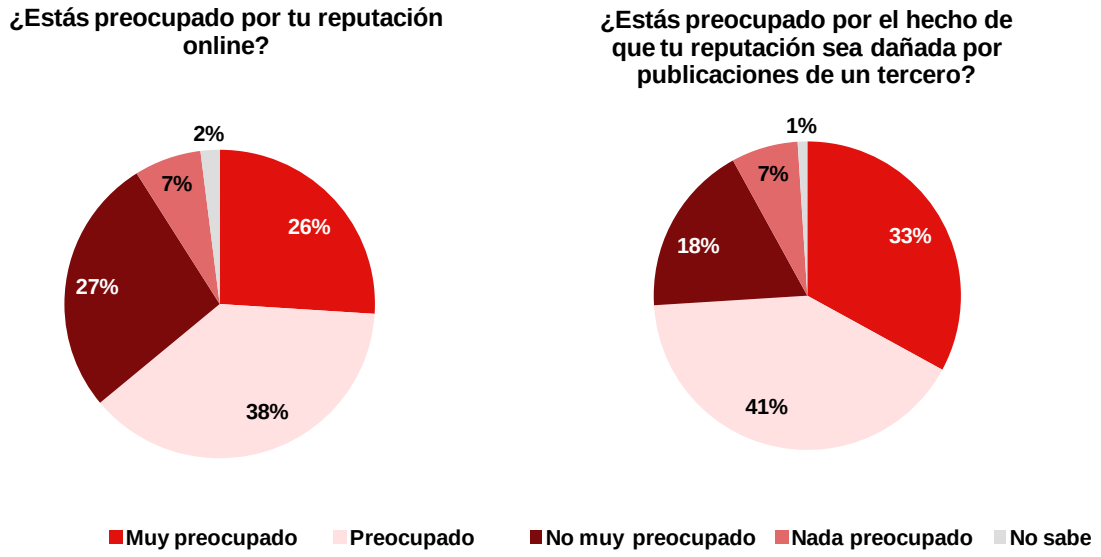
n=500 usuarios de Internet españoles (18-74 años) **Fuente: Microsoft (2012)**

3.2.4 La reputación online de los niños y adolescentes

En el contexto de la identidad digital y reputación online, es interesante prestar atención a los comportamientos de los niños y adolescentes. Estos, también denominados nativos digitales "viven" en Internet, esto es, desarrollan gran parte de su actividad y van creando su personalidad digital en las redes sociales, servicios de mensajería instantánea, plataformas educativas, videojuegos online, etc. Se trata de un colectivo más proclive a compartir información personal, y por ello son más laxos los límites a su privacidad que se autoimponen.

¿Qué opinan los menores españoles (8-17 años) sobre su reputación online? Los resultados no difieren demasiado de los que muestran los adultos. Si bien es cierto que el nivel de preocupación de los menores por su reputación online es ligeramente más bajo que el manifestado por los adultos, también se cumple la premisa de que les preocupa más el efecto que puede tener sobre su reputación las publicaciones realizadas por terceras personas.

Gráfico 4 Preocupación de los menores españoles (8-17 años) usuarios de Internet por su reputación online (%)



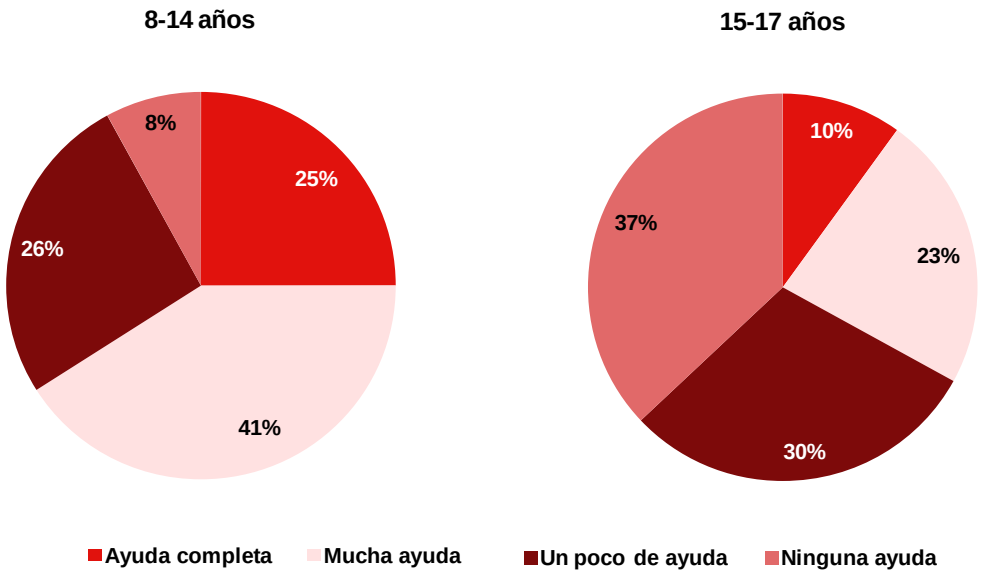
n=500 usuarios de Internet españoles (8-17 años) **Fuente: Microsoft (2012)**

Es evidente la existencia de una responsabilidad social que debe obligar a padres y comunidad educativa a proporcionar a niños y jóvenes tanto valores como pautas de actuación que contribuyan a un desarrollo armónico de la personalidad y a la construcción de una reputación online positiva y satisfactoria.

Los más pequeños son los que reciben más ayuda de sus padres para gestionar su imagen en Internet, mientras que en la adolescencia, la implicación del adulto es cada vez menor. Así, un 37% de los adolescentes españoles de entre 15 y 17 años reconocen no recibir ningún tipo de ayuda por parte de sus padres en la gestión de su identidad y reputación online. En el caso de los niños y niñas más pequeños (hasta 14 años), solo el 8% afirma no obtener refuerzo de sus progenitores en cuanto a la construcción de una reputación digital sólida.

En este punto, no está de más traer a colación la reflexión sobre si los padres y madres de los nativos digitales poseen las suficientes conocimientos y herramientas para proporcionar a sus hijos pautas sólidas para un comportamiento responsable en línea.

Gráfico 5: Ayuda que los hijos reciben de los padres en cuanto a la gestión y protección de la reputación online (%)



n=500 usuarios de Internet españoles (8-17 años) **Fuente: Microsoft (2012)**

4. Riesgos en la gestión de la identidad digital y reputación

Se describen a continuación los principales riesgos a los que se exponen las personas en relación a su identidad digital y reputación online.

Es importante destacar que las situaciones que provocan un impacto negativo en la vivencia online derivan en diferentes amenazas que aparecen entrelazadas, por lo que un mismo riesgo se puede contemplar desde diferentes perspectivas.

4.1 SUPLANTACIÓN DE LA IDENTIDAD DIGITAL

Caso 1: Como cada día, Raquel se dispone a utilizar su cuenta en Twitter, pero al introducir sus datos, la contraseña aparece como inválida y el acceso denegado. Su preocupación es todavía mayor cuando Raquel hace una búsqueda de su nombre en el buscador de la red social y descubre que alguien se está haciendo pasar por ella, publicando comentarios en su nombre. Esta "falsa Raquel" ha accedido al perfil y ha cambiado la contraseña para que su legítima dueña no pueda acceder al perfil.

En este caso, se ha producido una **suplantación de su identidad digital**, es decir, otra persona malintencionada se ha apropiado indebidamente de su identidad digital y ha actuado en su nombre. Dentro de este riesgo se contemplan varias situaciones:

- Registrar un perfil falso, sin utilizar información personal de la persona suplantada. Por ejemplo, perfiles caricaturizados de personajes públicos, que juegan con la confusión al utilizar nombres de usuarios muy similares al oficial, e incluso imágenes de perfil de la persona suplantada. Ejemplos destacados son los perfiles caricaturizados de personajes políticos[5].

- Crear un perfil falso, utilizando datos personales de la víctima. Por ejemplo, un periodista italiano creó perfiles falsos de escritores famosos, llegando a publicar informaciones falsas, como la supuesta muerte de Gabriel García Márquez anunciada en el perfil falso de Umberto Eco[6].

- Acceder de forma no autorizada al perfil de la víctima en un servicio de Internet para hacerse pasar por él. El caso de partida es un ejemplo de esta situación.

[5] Fuente: Caricatura 2.0. Fuente: http://www.legaltoday.com/practica-juridica/penal/nuevas_tecnologias/caricatura-20

[6] Fuente: *El falso Vargas Llosa es Tommaso Debenedetti*. Disponible en: http://cultura.elpais.com/cultura/2011/03/03/actualidad/1299106810_850215.html

En cada una de estas situaciones, será necesario estudiar la vulneración de los derechos del individuo: al honor y propia imagen, así como a la protección de datos personales (en este caso, sólo afecta a los dos últimos supuestos, puesto que en el primero no se produce esta divulgación).

La finalidad más inmediata del atacante es alterar la identidad sin consentimiento para perjudicar la imagen y reputación online. Pero también existen otros objetivos, como el robo de información personal, como paso previo para cometer ataques de fraude online, envío de correo spam o incluso divulgación de información falsa o descalificativa.

Las consecuencias de ser víctima de suplantación de identidad incluyen: mostrar una imagen distorsionada de sí mismo en Internet; ser víctima de burlas, insultos o amenazas, tener un descrédito frente a otros; sufrir una pérdida económica, etc.

4.2 AMENAZAS PARA LA PRIVACIDAD

Al participar en medios sociales, el individuo utiliza y difunde informaciones más o menos sensibles, que le caracterizan frente a los demás. Desde el momento en que se publica una información, se pierde el control sobre su difusión, por lo que puede acabar en manos de otras personas que hagan un uso inadecuado de la misma.

Bajo la categoría *Amenazas a la privacidad* se incluyen todas aquellas situaciones que impiden al individuo controlar de forma efectiva los datos de carácter personal vinculados a sus perfiles online.

En este control se incluye:

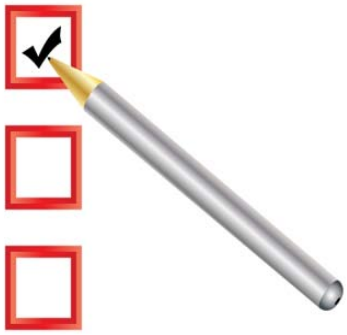
- La recogida de datos personales por las plataformas de Web 2.0 y servicios asociados (aplicaciones, etc.).
- La visibilidad que se hace de esa información.

A continuación se describen las principales situaciones que suponen una amenaza para la identidad digital desde el punto de vista de la privacidad.

4.2.1 Configuración insuficiente de las opciones de privacidad de la plataforma

Caso 2: Pedro tiene un perfil en Facebook donde comparte comentarios y fotos sobre sus gustos y aficiones, sin aplicar ninguna configuración de privacidad (es decir, permitiendo que todo el mundo pueda ver dicha información). Esto provoca que sus compañeros de trabajo conozcan detalles sobre su vida privada que en otras circunstancias Pedro nunca les revelaría.

Se contempla en este punto el riesgo de no acotar suficientemente la cantidad o el tipo de información que se muestra a los demás a la hora de utilizar redes sociales, blogs, etc.



Las opciones de privacidad por defecto que proporcionan las plataformas colaborativas pueden no ser suficientes a la hora de mostrar información. Esto puede desembocar en que otras personas conozcan detalles sensibles sobre las personas y puedan utilizarlos para dañar su imagen o reputación online. Como ocurre en el caso planteado, la información relativa a la faceta íntima de Pedro, fuera de ese contexto, puede generar una respuesta negativa en otro ámbito, como el profesional.

Para que esta difusión se haga de una forma adecuada y conforme a las preferencias del usuario es necesario ajustar las opciones de privacidad y filtrar qué información ve el resto de internautas (amigos, conocidos, otros internautas). Esta actuación es recomendable en varios momentos:

- Al registrarse en el servicio, puesto que en este momento el usuario otorga el consentimiento a unas condiciones específicas de privacidad (que ofrece la plataforma por defecto).

- Al utilizar el servicio, estableciendo filtros que permitan mostrar a cada destinatario la información adecuada. Por ejemplo, creando grupos diferenciados de amigos, familiares o compañeros de trabajo.

- Siempre que las plataformas actualicen y/o modifiquen sus políticas de privacidad, puesto que estas modificaciones pueden influir en la configuración establecida.

4.2.2 Alteración de la privacidad derivada de la sincronización entre plataformas

Caso 3: A Luis le gusta escuchar Spotify y ha dado permiso para que este servicio interactúe con Facebook. Además de las canciones que escucha, en su perfil de la red social se muestra información que afecta a su privacidad, como su ubicación geográfica, que si bien en principio no estaba habilitada en Facebook, ahora sí al sincronizarse ambas plataformas.

El uso de aplicaciones, juegos o sitios web vinculados a plataformas colaborativas puede implicar un cambio en las opciones de privacidad configuradas en los perfiles o páginas personales, que a su vez es susceptible de derivar en la divulgación de información sensible (por ejemplo, en el caso de partida descrito, datos sobre geolocalización[7]). Asimismo, la información personal que intercambia el usuario con su círculo puede ser utilizada por sus contactos cuando utilizan una aplicación social, con lo que, intencionadamente o no, los datos pueden circular más allá del entorno más cercano.

De nuevo, la falta de control en la difusión de información puede implicar una imagen digital distorsionada de la persona e impactar en su reputación.

Esta amenaza está muy ligada al uso de aplicaciones sociales en dispositivos móviles, puesto que al instalar estas apps se puede dar permiso para que se modifiquen las opciones de privacidad previamente configuradas. Por ejemplo, al instalar una app para utilizar Facebook en nuestro smartphone, esta nos solicita el uso de nuestros datos de geolocalización y los muestra en nuestro muro.

Por tanto, es importante que revisemos la configuración de privacidad, tanto desde la plataforma, como desde la aplicación:

- Desde la red social, revisando la configuración para controlar la información que se comparte con aplicaciones, juegos y sitios web por el usuario y sus contactos.
- Desde la aplicación, especialmente en el momento de su instalación, analizando qué información se intercambia y muestra en la plataforma vinculada.

[7] Por ejemplo, cabe citar entornos como Foursquare donde los usuarios marcan sitios (https://es.foursquare.com/). Chatroulette, en el que se desarrollan chats aleatorios con indicación de la localización mediante Chatroulette Map (http://chatroulette.com/), o las posibilidades de compartir localización con Google Latitude (http://www.google.com/intl/es/mobile/latitude/).

4.2.3 Riesgos del etiquetado en imágenes

Caso 4: María ha sido etiquetada junto a más gente en una foto de la fiesta de su facultad. La foto aparece en un post con el título "Botellón en la facultad". María acude a una entrevista de trabajo y el entrevistador le confiesa que ha visto esa foto al buscar más detalles sobre su formación académica, lo que le supone un gran bochorno y la pérdida de una oportunidad de trabajo. María quiere que la des-etiqueten de la foto.

La imagen en Internet es uno de los elementos de la identidad digital que más caracterizan a la persona, puesto que muestra el aspecto físico y permite a los demás reconocerle. Esta es una información especialmente sensible, puesto que una foto o vídeo sacados de contexto o en manos de terceros pueden influir negativamente en la identidad y reputación en la Red.

En este sentido, cada vez es más frecuente en los servicios de Web 2.0 la posibilidad de utilizar tecnologías de etiquetado, que permiten añadir metadatos a dichas imágenes. La acción de los buscadores puede implicar que las imágenes etiquetadas traspasen el círculo de contactos autorizados, llegando a disposición de terceros, que pueden utilizarlas de forma inadecuada.

4.2.4 Sexting

Caso 5: Rubén quiere dar una sorpresa a su chica y le envía una foto "sexy". Ella envía la foto a sus mejores amigas a través de su perfil en Tuenti y, aunque les pide que no la enseñen a nadie, una de ellas lo reenvía. Al día siguiente, todo el instituto ha visto la foto de Rubén, lo que genera burlas y humillaciones de todos sus compañeros.

Otra situación de riesgo ligada a la difusión de la imagen personal en Internet es la relativa al sexting. Bajo el término sexting se incluye la publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, que han sido creados voluntariamente por su autor, utilizando para ello el teléfono móvil u otro dispositivo tecnológico. Desde el momento en que este contenido se reenvía, el autor pierde el control, pudiendo tener una difusión ilimitada (por reenvío masivo, viralidad de los contenidos en redes sociales, etc.).

Por tanto, la divulgación no controlada de fotos o vídeos con contenido sexual afecta a la identidad digital y a la reputación online, al mostrar una faceta muy íntima y provocar, quizás, respuestas no deseadas de terceros. Esta conducta afecta especialmente a los adolescentes, en el que concurren una serie de circunstancias que lo hacen más vulnerable: mayor predisposición al riesgo, inicio de su desarrollo sexual y utilización generalizada de Internet (que permite inmediatez en las comunicaciones).

4.2.5 Uso de cookies sin conocimiento del usuario

Caso 6: Virginia ha estado visitando varias páginas web de búsqueda de empleo. A continuación, recibe en su correo electrónico Gmail y en su perfil de red social Google+ numerosas ofertas de trabajo. Virginia no recuerda haberse inscrito en esas ofertas y sospecha que pueden ser falsas. Además, otros contactos reciben estas ofertas de trabajo de forma masiva.

Un riesgo relacionado con la identidad digital radica en la posibilidad de que sitios web que el usuario visita utilicen cookies que permitan conocer cuál es la actividad del usuario dentro del sitio. Mediante estas herramientas pueden acceder a detalles como la localización del usuario, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de *clics* realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la Red. La finalidad de las cookies es hacer la navegación más sencilla, por ejemplo, proporcionando accesos rápidos a las secciones ya visitadas en una página web. El usuario tiene la posibilidad de configurar su navegador para ser avisado de la recepción de cookies y para impedir la instalación en su equipo.

Las cookies tienen implicaciones para la privacidad, ya que almacenan información susceptible de ser vulnerada por programas espía que la utilicen con fines malintencionados. Una vez que la información está en manos de atacantes, se pueden provocar ataques, por ejemplo, vendiendo esa información a terceros que envíen publicidad dirigida.

4.2.6 Privacidad de terceras personas.

Caso 7: Elena publica en su blog una entrada relatando la excursión que hizo con un grupo de amigos. En ella, ofrece detalles personales sobre la gente con la que ha ido, además de incluir fotos. Esto le ha supuesto un disgusto, puesto que uno de los participantes en dicha excursión no quería que esta actividad fuera conocida.

Al igual que la información sensible que una persona difunde sobre sí misma la caracteriza y genera una opinión en los demás, el hecho de hacer públicos datos de otras personas provoca un efecto en la imagen y reputación online de estos terceros.

El riesgo existe incluso cuando esta difusión se realiza en un entorno aparentemente cerrado en el caso de que, por cualquier circunstancia (re-difusión, etiquetado), esta información salga de ese círculo. En consecuencia, el propietario de los datos podría exigir responsabilidades.

4.3 AMENAZAS A LA REPUTACIÓN ONLINE

Las amenazas a la reputación online son aquellas situaciones que pueden menoscabar la opinión o el prestigio que una persona ha adquirido en su vivencia online. Estas circunstancias se pueden producir:

- Por la propia actuación del individuo, puesto que en medios sociales aumenta la visibilidad de las actuaciones.
- Por la actuación de terceros que publican información sobre el sujeto, combinada con la acción de servicios como los buscadores.
- Por la actuación de los demás internautas con los que nos relacionamos.

El riesgo a sufrir un impacto en el honor o la reputación aumenta en Internet, ya que la viralidad en la difusión de los contenidos dificulta el control por parte del propietario de la información personal. Esta información puede terminar en manos de terceros que la utilicen de forma inadecuada.

A continuación se exponen las principales situaciones que suponen una amenaza a la reputación de un individuo ligada a su presencia online.

4.3.1 Impacto de las publicaciones que exceden a la libertad de información

Caso 8: Ana se encuentra disfrutando de unas vacaciones en la playa y coincide en el mismo hotel con un actor famoso. Ana toma fotos de este actor y las sube a su blog, comentando a su vez detalles como el hotel en el que se alojan o quién le acompaña.

A la hora de utilizar las páginas y perfiles personales como medio de expresión, las personas ejercen el derecho a la libertad de información. Sin embargo, este derecho tiene unos límites legales, que marcan la frontera entre lo que atenta contra la reputación o no.

Para publicar libremente, es importante asegurar que los hechos o personas de quien se habla son ciertos y de relevancia pública. Pero a la vez, se debe respetar el espacio íntimo de las personas, incluidas aquellas de notoriedad pública.

4.3.2 Daño reputacional debido a publicaciones falsas, injurias y calumnias

Caso 9: Julián tiene un blog en el que trata de compartir parte de sus conocimientos y experiencias como dentista de niños. Otros usuarios publican comentarios que le imputan delitos falsos, como realizar fraude en su actividad. Este hecho hace que la clientela descienda.

Nada en Internet impide que, en aplicación de la libertad de expresión, aparezcan en la Red informaciones erróneas (sin un propósito malintencionado), injurias (información manifiestamente falsa) o calumnias (imputación de delitos falsos) sobre una persona, que constituyan un ataque al honor y la reputación de la misma.

Los proveedores del servicio, esto es, quienes alojan el blog o la red social, no son responsables de los contenidos y solo pueden actuar retirándolos o bloqueándolos cuando tengan conocimiento efectivo de los mismos. Para ello, suelen disponer de canales de denuncia a disposición de los usuarios.

A pesar de las medidas reactivas que se pueden aplicar (retirada de los comentarios, acciones legales, etc.), la capacidad de difusión en medios sociales aumenta el daño sobre la imagen que tiene la persona de cara a la comunidad internauta. En el ejemplo inicial, dichos comentarios pueden acarrear el fin de la carrera profesional de Julián si la difusión de dicha información implica la pérdida de confianza de sus clientes.

4.3.3 Informaciones descontextualizadas

Caso 10: En 2009 Sofía fue multada por sobrepasar la velocidad permitida con el coche. A pesar de que han pasado varios años desde el incidente, la información sobre la sanción sigue apareciendo en los buscadores de Internet. Sofía es ahora profesora de autoescuela, y esta información claramente repercute de forma negativa en su imagen profesional.

La acción de los buscadores, que permiten visualizar informaciones pasadas sobre una persona en Internet, genera la amenaza de descontextualización y pérdida de sentido de una publicación. Esta permanencia de la información implica la continuidad del impacto negativo en la reputación de dicha persona, e incluso de sus familiares[8].

Por ello, en la actualidad la sociedad reclama un "derecho al olvido" en la Red.

[8] Véase, por ejemplo, el caso Moreno vs. Hanford Sentinel, Inc. et al, disponible en http://www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=11&idioma=english.

4.3.4 Utilización no consentida de derechos de propiedad intelectual

Caso 11: Alberto tiene una página personal, en la que utiliza imágenes que encuentra en Internet. Alberto recibe una denuncia por utilizar un vídeo creado por otra persona sin atender a los acuerdos de uso del mismo. Este hecho no es ajeno al prestador del servicio en el que Alberto tiene alojado su página, y poco después comunica a Alerto el cierre de este espacio personal.

Utilizar materiales de terceros (textos, imágenes, vídeos) sin atender a los derechos de propiedad intelectual puede desembocar en una situación de amenaza para la reputación online, tanto del autor de la obra como del que la utiliza sin consentimiento:

- El autor ve menoscabada su reputación, puesto que parte de la valoración sobre su obra se diluye.
- El individuo que utiliza obras sujetas a derechos de autor en Internet está, a su vez, dando visibilidad al acto ilícito, lo que muy probablemente desemboque en valoraciones negativas o acciones legales de respuesta por parte del autor.

No existe prohibición de publicar contenidos en los siguientes casos:

- Cuando se haga alusión a noticias, siempre que se haga referencia a la fuente y no se copie literalmente sin permiso de sus titulares.
- Cuando sea una reproducción parcial como cita que ilustra un *post*, siempre que se reconozca la autoría.
- Cuando los materiales no estén sujetos a derechos de autor. En este caso, se podrían reproducir íntegramente.

5. Marco legal

En la Sociedad de la Información, la identidad digital personal y la reputación online constituyen elementos valiosos y merecedores de protección jurídica.

Al igual que ocurre en el Derecho internacional, no existe en la Constitución Española un reconocimiento expreso del derecho a la identidad (e identidad digital), sino que se vincula de modo ineludible a los derechos de la personalidad.

El Tribunal Constitucional ha articulado la protección de los signos que caracterizan la identidad y reputación de las personas a través de los derechos del art. 18 de la Constitución Española y, singularmente, a través de la tutela de la imagen y el honor, y del derecho fundamental a la protección de datos.

A continuación se estudian los derechos individuales aplicados a la vivencia online de las personas, deteniéndose en las implicaciones jurídicas que pueden tener determinadas acciones relacionadas con el menoscabo de la identidad digital y reputación online.

Asimismo, se incluye la responsabilidad que tienen los prestadores de servicios de Web 2.0 para asegurar una convivencia online adecuada y respetuosa entre sus usuarios.

5.1 DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y FAMILIAR Y A LA PROPIA IMAGEN

La Constitución española reconoce en el artículo 18 los derechos al honor, a la intimidad personal y familiar y a la propia imagen. Estos derechos protegen la dimensión subjetiva de la personalidad, que depende de la propia actuación, pero también la dimensión social, que se refiere a cómo participan los demás en estos actos y generan una determinada reputación. Estos derechos asisten al individuo también en su plano digital.

En concreto:

- **Derecho al honor.** Puede definirse como el aprecio o estima que una persona tiene en un contexto social determinado. En Internet este derecho protege a la persona frente a agresiones como la publicación de noticias u opiniones que lo hagan desmerecer socialmente.

- **Derecho a la intimidad**. El derecho protege una esfera privada de la cual el individuo puede libremente excluir a terceros, e impedir intromisiones en un ámbito reducido de relaciones personales. En el ámbito de servicios como las redes sociales, la intimidad de los usuarios puede verse fácilmente vulnerada, puesto que las informaciones traspasan con frecuencia el círculo de relaciones personales del titular, saliendo del anonimato.

- **Derecho a la propia imagen**. El Tribunal Constitucional ha determinado[9] que este derecho protege los *atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre*. El derecho a la propia imagen confiere un poder de disposición respecto de cualquier uso que terceros quieran realizar de estos atributos, ya que se requiere el consentimiento del afectado. En la práctica, desde el momento que cualquier información se publica en la Red, incluida la imagen personal, el individuo pierde el control sobre ella.

Estos derechos pueden tutelarse mediante las acciones ejercitables conforme a 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.

5.1.1 Derecho de información y libertad de expresión *versus* derecho a la propia imagen, a la intimidad y al honor

Una de las aportaciones más significativas de la Web 2.0 ha sido democratizar el ejercicio del derecho a la información y la libertad de expresión recogidos en el artículo 20 de la Constitución. Esto provoca la transferencia de una parte sustancial de la reputación personal al resto de usuarios a través de canales colaborativos.

Para influir positiva o negativamente en la reputación online, basta la creación de un blog, un grupo de Facebook o simplemente dejar un comentario positivo o negativo en un panel de discusión: todo será automáticamente registrado en el "Internet Archive" y en la memoria de los motores de búsqueda, permitiendo además que el comentario o información perduren en el tiempo. A diferencia de la prensa, Internet no necesita asegurar la veracidad de los hechos antes de publicarlos, por lo que los usuarios pueden crear datos falsos sin interferencias.

La libertad de información permite a las personas publicar noticias, siempre que las informaciones sean ciertas, es decir, que hayan sido verificadas o comprobadas y que tengan relevancia pública, derivada de la importancia social de la noticia. La relevancia puede venir dada por el interés de la persona objeto de la noticia.

Por su parte, **la libertad de expresión**: se refiere a la publicación de pensamientos, ideas u opiniones, que suponen una valoración subjetiva de la realidad.

[9] Véase STC 117/1994.

El ejercicio de estas libertades, especialmente de la libertad de expresión, puede chocar con los derechos de la personalidad (al honor, intimidad y propia imagen) que asisten a todos los individuos fuera y dentro de Internet, con el factor añadido del poder de difusión de los contenidos en este medio, que puede ampliar los efectos negativos de un ataque a estos derechos. Por ello, existen unos límites a la publicación de información.

El primero de los límites es respetar la dignidad de las personas y no atentar contra ella por medio de la calumnia o la injuria. Estas figuras, que forman parte de los delitos de prensa, se aplican igualmente en Internet, teniendo en cuenta que quien propaga una información se convierte en "difusor" de la misma, pudiendo dañar la imagen de una persona a la cual muchas veces ni siquiera conoce.

- **La calumnia** consiste en *la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad (*artículo 205 del Código Penal*).*

- **La injuria** *es la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación (*artículo 208 del Código Penal*).*

En segundo lugar, la intimidad de cada usuario es una barrera cada vez más débil a favor de lo público. De hecho, el principio de las redes sociales es animar a los usuarios a compartir información sobre su vida privada y generar conversación, redistribuyendo y diluyendo informaciones privadas de otros más allá del grupo de contactos directos del titular de la información.

Especialmente relevante es la afección a la intimidad y la propia imagen a través de la publicación de fotografías, puesto que a menudo se realiza sin el consentimiento ni consulta de la persona representada.

En este sentido, en la práctica resulta casi imposible mantener el control sobre la imagen pública a través de Internet. Esto plantea la cuestión de la violación del derecho a la imagen por parte de los motores de búsqueda como Google Imágenes, que reproducen las fotos e imágenes en Internet que corresponden a una búsqueda. Los mismos problemas se encuentran en las redes sociales, en que todos facilitan la publicación y reproducción de las fotografías de todo el mundo.

Por último, a la hora de utilizar materiales de terceros sin autorización el límite lo constituyen los derechos de autor que puedan afectar a la obra en cuestión, con el consiguiente daño a la reputación online del creador. En este sentido:

- Es lícito hacer alusión a noticias de terceros y publicar referencias citando el origen (reportaje neutral). Así, se puede elaborar un post sobre un tema tratado en la prensa, pero no copiar literalmente noticias sin permiso de sus titulares.

- Puede reproducirse parcialmente un texto, por ejemplo como cita que ilustra un post, siempre que se reconozca la autoría. No se permite la reproducción íntegra de materiales ajenos, salvo que no estén sujetos a derechos de autor.

- No está permitido reproducir libremente cualquier fotografía obtenida en Internet, ya que puede estar sujeta a derechos de autor.

Las consecuencias de un inadecuado conocimiento de las responsabilidades jurídicas en el ejercicio de la libertad de información y expresión en la Web 2.0 pueden traducirse en la exigencia de indemnizaciones por los perjuicios eventualmente causados a los derechos al honor, la intimidad personal y familiar y la propia imagen y/o a la propiedad intelectual.

No debe olvidarse que los proveedores del servicio, esto es, quienes alojan el blog o la red social, no son responsables de los contenidos y no podrán actuar retirándolos o bloqueándolos hasta que no tengan conocimiento efectivo de los mismos. Por tanto, hay que verificar si el servicio posee un mecanismo de denuncia y utilizarlo adecuadamente.

5.2 EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

El derecho a la protección de datos es el derecho que tiene todo ciudadano a controlar sus datos personales y a disponer y decidir sobre los mismos. Se trata de un derecho fundamental con entidad propia y diferente al derecho a la intimidad.

A nivel europeo, la Directiva 95/46/CE es la norma de referencia en materia de protección de datos. En España, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y su reglamento de desarrollo (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 de Carácter Personal, RDLOPD) conforman la base legal para la protección de datos.

¿De qué hablamos cuando decimos “dato personal”? Constituye un dato personal *cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo concerniente a personas físicas identificadas o identificables*. Según esta definición el nombre, la dirección, los datos de contacto, el curriculum vitae, el salario, una fotografía o un vídeo constituyen datos de carácter personal.

La normativa sobre protección de datos proporciona a los sujetos titulares de los datos personales una serie de derechos:

- **Derecho de acceso.** En virtud del derecho de acceso, regulado en el art. 15 de la LOPD, el ciudadano puede solicitar y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, así como el origen de dichos datos y las comunicaciones realizadas o que se prevean realizar.

- **Derecho de rectificación.** El art. 16 de la LOPD reconoce al ciudadano el derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales, en el caso de que éstos sean inexactos o incompletos. La solicitud de rectificación debe indicar el dato que se estima erróneo y la corrección que debe realizarse y debe ir acompañada de la documentación justificativa de la rectificación solicitada.

- **Derecho de cancelación**. Este derecho, regulado en el art. 16 de la LOPD, ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales.

- **Derecho de oposición.** El ciudadano puede oponerse, mediante su simple solicitud, a que sus datos sean tratados con fines de publicidad y de prospección comercial. Este derecho de oposición se encuentra regulado en los arts. 6.4, 17 y 30.4 de la LOPD. Se ejercita mediante una solicitud por escrito dirigida al responsable del fichero o tratamiento, en la que se hagan constar los motivos fundados y legítimos relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

Además, la normativa sobre protección de datos obliga al responsable del fichero o tratamiento a informar a los titulares de la incorporación de sus datos a un fichero, de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

El deber de consentimiento, por su parte, implica la obligación de solicitar el consentimiento explícito de las personas físicas titulares de los datos - antes de la recogida de los mismos - para proceder al tratamiento. El consentimiento se debe establecer mediante un mecanismo claro cuya opción de recogida no esté validada por defecto.

El usuario de Internet que proporcione sus datos personales en un formulario online con objeto de, por ejemplo, darse de alta en una red social, es informado de la existencia y finalidad de un fichero en el momento del registro (normalmente, esta información se encuentra dentro de la política de privacidad). A continuación, mostramos un extracto de la política de privacidad de la red social Tuenti[10], donde se da cumplimiento al deber de información.

[10] www.tuenti.com Extracto de las condiciones de privacidad vigentes el 18 de mayo de 2012.

Nuestra Política de Privacidad afecta tanto a la información personal que nos proporcionas al crearte un perfil como a todos los datos que nos facilites al acceder a cualquiera de los servicios disponibles en la plataforma de TUENTI, durante el tiempo que tengas un perfil.

Los datos que aportas a TUENTI son incluidos en nuestros ficheros registrados ante la Agencia Española de Protección de Datos (AEPD).

TUENTI recoge y trata tus datos para identificarte como usuario de la plataforma de TUENTI y para darte acceso a los servicios, funcionalidades y aplicaciones que ponemos a tu disposición.

Recuerda que puedes oponerte en cualquier momento a recibir comunicaciones de TUENTI para fines comerciales y promocionales, incluyendo por medios electrónicos, contactándonos a través de unsubscribe@tuenti.com.

Como usuario de TUENTI tienes derecho a acceder a tus datos personales para saber cómo los tratamos y con qué finalidad y decirnos si no quieres que usemos tus datos para una actividad concreta. Además, podrás rectificar cualquier error en tus datos si ves que no son correctos e incluso podrás pedirnos que los cancelemos si quieres dejar de ser usuario de la plataforma de TUENTI.

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español es, con carácter general, la Agencia Española de Protección de Datos (AEPD).

5.3 EL DERECHO AL OLVIDO

En Internet se conforman de manera constante biografías digitales que son alimentadas por las aportaciones del sujeto en cuestión que, de manera consciente, construye su identidad digital. A este componente consciente y responsable del individuo hay que añadir las publicaciones generadas por terceras personas, que en ningún caso han sido consentidas por el personaje.

> Puede definirse el **derecho al olvido** como la facultad que se atribuye al individuo de obtener la eliminación de una determinada información, particularmente en el contexto de Internet.

Basta con poner el nombre de una persona entre comillas en un buscador y éste ofrecerá un completo perfil de la información que sobre él o ella circula en la Red. Si el individuo es aficionado a las carreras populares, podremos conocer en cuáles ha participado, e incluso cuál ha sido su marca personal. Si se le ha concedido una subvención o beca, podremos acceder a esos detalles.

En estos momentos, el ciudadano únicamente tiene a su disposición las herramientas que le facilita el derecho fundamental a la protección de datos. En ocasiones estas herramientas son insuficientes, ya que existe un conflicto en los siguientes ámbitos:

- Publicaciones oficiales, que por su propia naturaleza están orientadas a dotar de publicidad a determinadas situaciones. Se trata, por ejemplo, de las contenidas en boletines y diarios oficiales.

- Buscadores en Internet que, como servicios de la sociedad de la información, en principio juegan un papel neutral, y no responden por los contenidos de terceros.

- Medios de comunicación que publican noticias de interés público.

En España, y habitualmente ante la AEPD, se han planteado denuncias y solicitudes de tutela de derechos de cancelación frente a publicaciones en boletines oficiales de actos administrativos que incluían datos personales relevantes, o frente a páginas web y redes sociales. Adicionalmente las denuncias, y las correspondientes actuaciones de la Agencia, se han dirigido también contra los propios buscadores[11].

En el debate público aparecen dos posiciones enfrentadas: los que defienden un "derecho al olvido" para borrar de Internet determinada información personal, y los que argumentan que todo lo que existe en Internet pertenece a una especie de historia, y que como hechos históricos no pueden ser borrados ni desaparecer.

En el debate, aunque no resuelto definitivamente, las autoridades de la Unión Europea y la Agencia Española de Protección de Datos, defienden que la futura regulación europea del derecho fundamental a la protección de datos contenga una formulación expresa del derecho al olvido[12].

5.4 LA HERENCIA DIGITAL

La presencia de los individuos en el mundo digital puede mantenerse incluso después de su fallecimiento, generando nuevos rastros de identidad y de reputación online. Por ejemplo, el fallecimiento de Michael Jackson[13] generó una gran cantidad de conversaciones de la comunidad internauta en las páginas y perfiles personales del cantante.

[11] Puede verse a título de ejemplo las tutelas de derechos tramitadas respecto de buscadores como Yahoo (TD/00400/2011) o Google (TD/00833/2008). Pero también respecto de proveedores como Facebook y YouTube (TD/01239/2010) o un Boletín Oficial (TD/00637/2011).

[12] Versión no oficial de Statewatch (2011): "Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (General Data Protection Regulation). Disponible en:

http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf

[13] Más información: http://www.rtve.es/noticias/20090626/muerte-michael-jackson-bloquea-red/282433.shtml

Los prestadores de servicios de red social son sensibles a este hecho y ofrecen diversas opciones a las personas cercanas al fallecido. Por ejemplo, Facebook permite denunciar el perfil de una persona fallecida, o cerrar la cuenta si un pariente del usuario realiza una notificación formal. Además, es posible mantener un perfil conmemorativo de esta persona[14].

¿Qué ocurre con la información personal recogida en perfiles y páginas de Internet? Cada vez son más frecuentes los conflictos relacionados con el acceso y la toma de decisiones sobre estos datos, como parte de la herencia digital del fallecido a sus descendientes. El artículo 659 del Código Civil señala que *la herencia comprende todos los bienes, derechos y obligaciones de una persona, que no se extingan por su muerte*. Por tanto nada impide que los herederos puedan ejercer sus derechos ante quienes dispongan de información relativa a la identidad digital del fallecido.

Así, el cónyuge, los descendientes, ascendientes y hermanos de la persona y en última instancia el Ministerio Fiscal están facultados para solicitar la protección de estos derechos de la personalidad del fallecido, según establece el artículo 4 de la ley de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Además, los herederos pueden dirigirse a los responsables de los ficheros o tratamientos que contengan datos de este con la finalidad de notificar su muerte y solicitar, en su caso, la cancelación de los datos, como indica el artículo 2.4 del RDLOPD.

[14] Fuente: Francisco Pérez Bes (2011): "Difuntos 2.0: cómo gestionarlos". Disponible en: http://www.territoriocreativo.es/etc/2011/11/difuntos-2-0-como-gestionarlos.html

5.5 LA SUPLANTACIÓN DE IDENTIDAD

Los riesgos existentes en la suplantación de la identidad de otra persona han sido descritos en el apartado 4.1. Desde el punto de vista legal, el problema reside en la falta de tipificación penal de esta conducta, que inevitablemente se reconduce al delito de usurpación del estado civil del art. 401 del Código Penal: *el que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años*.

El Tribunal Supremo ha precisado los requisitos para que se cometa este delito: (…) *para usurpar no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden; como puede ser el obrar como si uno fuera otro para cobrar un dinero que es de este, o actuar en una reclamación judicial haciéndose pasar por otra persona, o simular ser la viuda de alguien para ejercitar un derecho en tal condición, o por aproximarnos al caso presente, hacerse pasar por un determinado periodista para publicar algún artículo o intervenir en un medio de comunicación* (FJ segundo de la STS núm. 635/2009 de 15 junio, de la Sala de lo Penal, Sección 1ª).

La carencia de una regulación penal adecuada se manifiesta con mayor intensidad en los actos derivados de la suplantación. De ahí que la doctrina penal considere aplicar distintos tipos de delito, como la estafa ordinaria (art. 248.1 CP); la estafa informática (art. 248.2 CP), los delitos contra la intimidad (art. 197 CP); o los delitos contra la propiedad intelectual e industrial y las falsedades documentales (arts. 270, 274 y 390 CP).

La Agencia Española de Protección de Datos ha abierto una vía útil para conseguir que los proveedores de servicios en Internet retiren la información y colaboren en la identificación de los suplantadores. Así, en el Procedimiento Sancionador PS/ 00137/2011[15] en el que una persona suplantó la identidad de otra en una red social, y habiendo identificado al suplantador mediante la información facilitada sobre la IP del ordenador desde la que ésta se produjo, la Agencia Española de Protección de Datos consideró que existía un tratamiento de datos personales y se vulneraba el principio del consentimiento del artículo 6.1 LOPD.

[15] Procedimiento disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2011/common/pdfs/PS-00137-2011_Resolucion-de-fecha-27-07-2011_Art-ii-culo-6.1-LOPD.PDF

5.6 LA RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS

Generalmente, los servicios utilizados en la llamada Web 2.0, como los blogs, las redes sociales, los gestores de imágenes y muchos otros recursos destinados a la gestión o agregación de contenidos, son prestados por terceros.

La responsabilidad de estos proveedores está delimitada por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), que traspone la Directiva 2000/31/CE de Comercio Electrónico. Ésta define un prestador como la persona física o jurídica que proporciona un servicio de la Sociedad de la Información y fija un régimen de responsabilidad para éstos.

Los proveedores son responsables en todos los órdenes (civil, penal o administrativo), de aquellas conductas realizadas directamente por ellos o por el personal a su servicio y que impacten en los derechos de los usuarios. Por ejemplo, en 2010 la AEPD abrió un procedimiento sancionador a Google por captar y almacenar datos personales de localización de redes wifi con identificación de sus titulares para su servicio Street View[16].

Sin embargo, en lo relativo a las conductas de los usuarios de sus servicios que dañan la imagen o reputación de otros, la legislación parte de ciertos principios básicos que determinan, en su caso, una exención de responsabilidad:

- El prestador no tiene ninguna obligación de supervisión o monitorización de los mensajes que circulan por medio de su servicio, de los datos o contenidos que se alojan en sus sistemas, ni de los hiperenlaces que incluyen los usuarios.

- El prestador no responde de contenidos o hiperenlaces ilícitos siempre que no tenga conocimiento efectivo de su existencia y actúe con diligencia retirándolos o haciendo imposible el acceso a los mismos en el momento en que tenga tal conocimiento (arts. 16 y 17 LSSI).

  El conocimiento efectivo, según esta ley, se produce cuando un órgano competente declara la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos. También se da cuando se declare la existencia de la lesión, y el prestador conozca la correspondiente resolución.

[16] Más información: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/octubre/101018_np_google.pdf

Ello sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores aplican en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que puedan establecerse. Por tanto, también puede existir un conocimiento de este tipo cuando existe una notificación del perjudicado y el proveedor es consciente de la ilicitud.

6. Recomendaciones para la gestión de la identidad digital

La identidad digital se ve afectada por la interacción del usuario con otras personas y depende en gran medida de su propia conducta. Por ello, resulta de utilidad conocer las pautas para la gestión de la vivencia en la Red y la respuesta ante impactos en dicha identidad y reputación online.

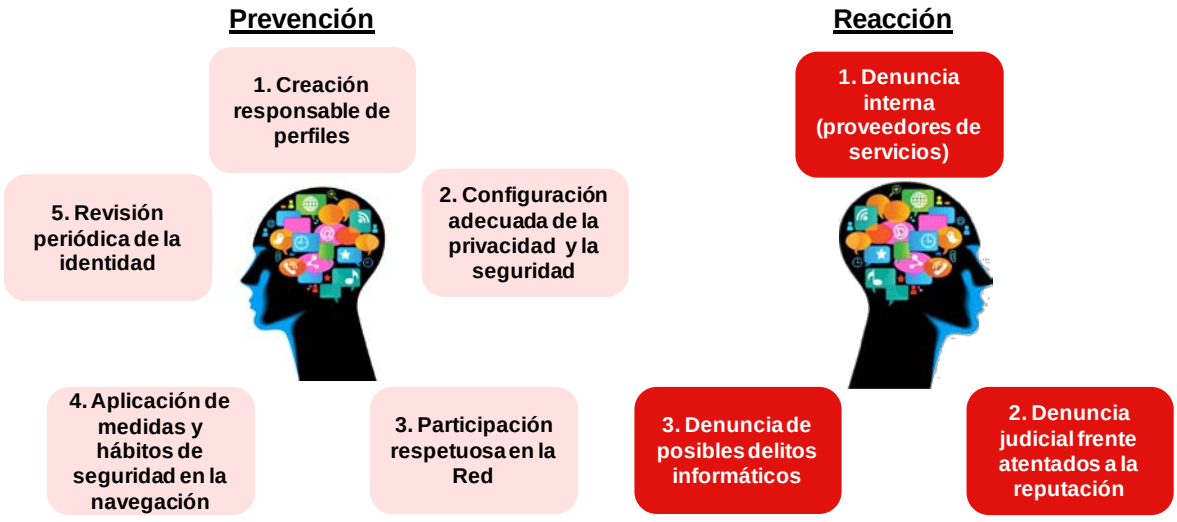
Además, existen ámbitos en los que la actuación de los poderes públicos o el compromiso de los proveedores de servicios pueden proporcionar las soluciones que la dinámica de Internet ha sido incapaz de proporcionar por sí misma.

6.1 RECOMENDACIONES DIRIGIDAS A LOS USUARIOS

El principal implicado en conformar una adecuada identidad digital y reputación online es uno mismo, mediante la gestión segura y responsable de los diferentes perfiles o identidades parciales que utilice en Internet, especialmente en las redes sociales.

Con independencia de las cautelas preventivas que se adopten, la interacción que se produce en las redes sociales multiplica las posibilidades de padecer algún tipo de ataque a la reputación. Cuando hay una vulneración de derechos el usuario puede acudir a diversos canales de denuncia, incluyendo los Cuerpos y Fuerzas de Seguridad del Estado, la Agencia Española de Protección de Datos, o los Tribunales de Justicia, en función de la infracción a denunciar.

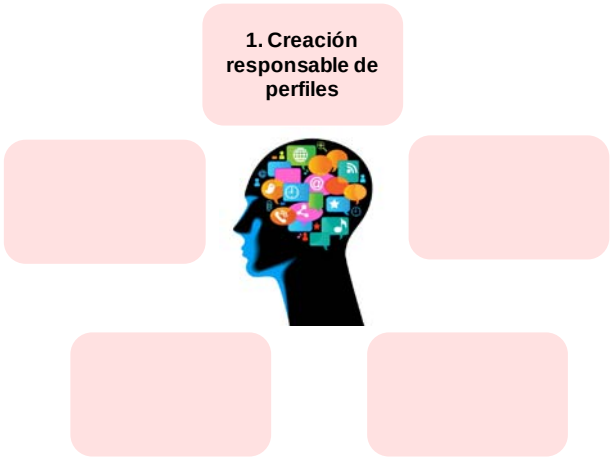
A continuación se exponen tanto las recomendaciones preventivas como reactivas dirigidas a usuarios para una correcta gestión de su identidad digital. A modo de resumen, en la siguiente ilustración se recogen cada una de las pautas básicas que se analizarán en los siguientes subapartados.



Recomendaciones de prevención y reacción dirigidas a usuarios para la gestión de la identidad digital

6.1.1 Recomendaciones preventivas

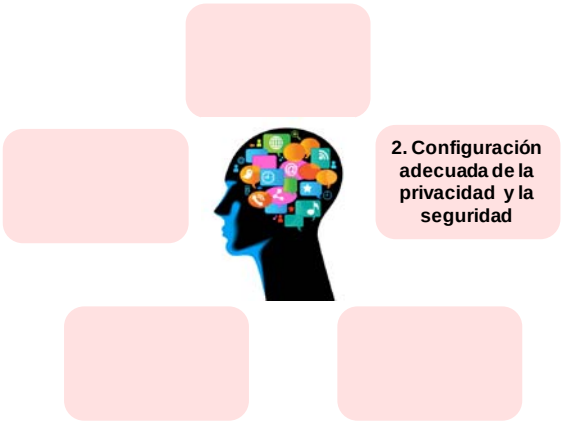
1) Creación responsable de perfiles



La decisión de crear un perfil de usuario o identidad parcial en un determinado servicio online (blog personal, perfil en red social, etc.) debe tener en cuenta las siguientes recomendaciones:

- Valorar previamente la utilidad que un servicio online va a reportar y las implicaciones que puede tener para la seguridad y privacidad de los datos personales.
- Comprobar, con carácter previo al registro, la finalidad del tratamiento de los datos personales por el proveedor del servicio, en qué consiste el tratamiento y las responsabilidades del usuario y el prestador del servicio.
- Establecer identidades digitales parciales (como perfiles separados) para la actuación personal y profesional, con el objeto de evitar difundir una imagen personal de forma inadecuada.

2) Configuración adecuada de la privacidad y la seguridad

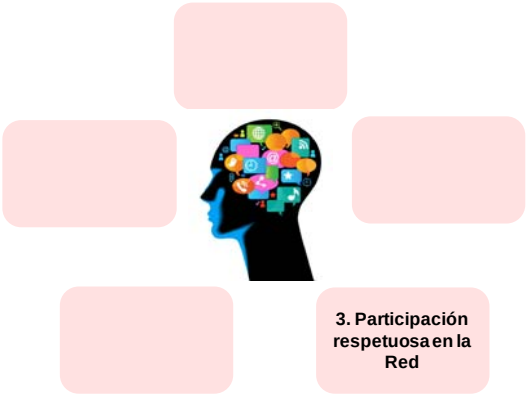


Una vez elegido el medio o servicio, el usuario debe aprender cómo funciona y configurar, en cada caso, las opciones de seguridad y privacidad de forma que se garantice al máximo el control de la información y las relaciones. En este sentido se recomienda:

- Configurar adecuadamente los parámetros de privacidad y seguridad[17] de la web social.
- Valorar la información que se publica antes de hacerlo, puesto que una vez que se lanza en la corriente social, se pierde el control sobre la misma.
    - Ser especialmente cautos con las fotografías o vídeos que se publican en Internet, ya que identifican físicamente al individuo.
    - Limitar el uso de datos de localización a aplicaciones estrictamente necesarias.
    - Adecuar el grado de divulgación de la información al tipo de relación con otros usuarios.
- Conceder acceso sólo a las aplicaciones de terceros que sean dignas de confianza, tratando siempre de limitar las publicaciones que las mismas realicen en el perfil o espacio personal.
    - Verificar al máximo quién es el titular de la aplicación a la que se autoriza el uso de datos de identidad, qué datos precisa y para qué los necesita.
    - Conceder a las aplicaciones acceso sólo a los datos imprescindibles, empleando los medios establecidos para ello por el proveedor.
- Cerrar adecuadamente la sesión en el perfil o servicio al terminar, para evitar que otros accedan al mismo y puedan utilizarlo con fines maliciosos.

[17] Para realizar esta configuración, se pueden consultar las Guías publicadas por INTECO en relación con doce servicios de red social, disponibles en http://www.inteco.es/Seguridad/Observatorio/guias/guia_ayuda_redes_sociales.

3) Participación respetuosa en la Red



En el momento en el que se está participando en un determinado servicio online se debe ser respetuoso con los demás individuos. Para ello algunas de las recomendaciones son:

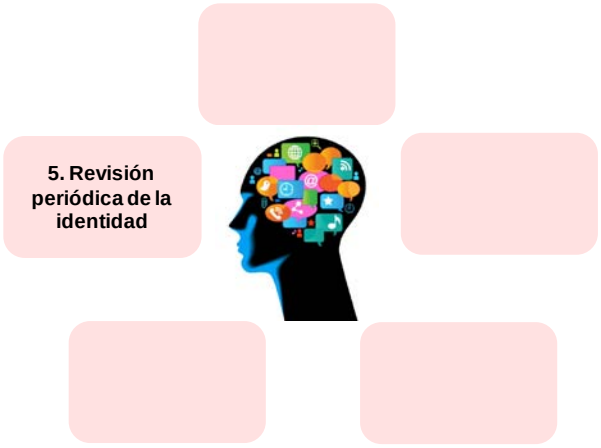
- Usar el sentido común a la hora de informar u opinar sobre un hecho concreto. Por ejemplo, se recomienda:
  - No utilizar un tono maleducado o vejatorio.
  - Aplicar un mínimo de tolerancia y empatía hacía los demás.
  - No publicar información falsa o advertir del tono de la misma.
- Solicitar siempre permiso antes de utilizar datos de otras personas, especialmente cuando se trate de fotos o vídeos. En particular, se debe ser especialmente respetuoso con el empleo de etiquetas en imágenes y videos de acceso público.
- Conocer, cuando proceda, las obligaciones jurídicas, los términos y condiciones o los códigos éticos del servicio a las que se pueda estar sometido y cumplirlos escrupulosamente.

4) Aplicación de medidas y hábitos de seguridad en la navegación

Con carácter general, es recomendable aplicar medidas y hábitos de seguridad en la navegación, previniendo que el equipo, las sesiones o los perfiles sean atacados y la información pase a manos de terceros. Para ello se recomienda:

- Disponer de software de seguridad en todos los equipos desde los que se actúa online y mantener actualizados estos programas.
- Comprender el empleo de las *cookies* del navegador y otros dispositivos de trazabilidad, y evaluar la posibilidad de desactivarlas, cuando resulte posible sin impedir el empleo del servicio en línea.
- Revisar el sistema de concesión de permisos a servicios de búsqueda de información y publicidad, y, en su caso valorar su desactivación.

5) Revisión periódica de la identidad



Resulta recomendable adoptar la práctica de realizar búsquedas frecuentes sobre la información personal en Internet para llevar a cabo un control preventivo, y en el caso que sea necesario adoptar medidas correctoras.

Asimismo, es aconsejable revisar los cambios en políticas de privacidad de cada servicio, ya que pueden afectar a la cantidad de información que se divulga públicamente. En caso de que esto ocurra, adaptar en consecuencia las preferencias de privacidad.

6.1.2 Recomendaciones reactivas

1) Denuncia interna (proveedores de servicios)

Habitualmente los proveedores de servicios de Internet disponen de sistemas de denuncia con la finalidad de salvaguardar los derechos de los usuarios y de terceros ajenos al servicio.

Así, cualquier persona que considere que su información personal se ha utilizado de forma indebida, puede solicitar el ejercicio de los derechos de acceso, rectificación, cancelación u oposición al tratamiento (ARCO) ante el prestador del servicio.

La persona se debe dirigir prioritariamente ante el origen de la publicación y, en el caso de que la información no desparezca de la memoria caché de los buscadores o siga en *websites* de terceros, se debe dirigir ante el buscador o ante aquellos que la hayan indexado.

Por su parte, los proveedores carecen de responsabilidad hasta que poseen conocimiento efectivo. Los canales de denuncia suelen ser muy eficaces a la hora de retirar la información y de bloquear usuarios. Pero normalmente, la retirada comporta el "borrado" de la información. Por ello resulta aconsejable:

- Hacer una captura de pantalla de la página que se desea rectificar o borrar, o de la conducta que se desea perseguir, en el que conste la dirección de Internet y la fecha. En cualquier caso, este tipo de documento constituye una prueba muy débil.
- Realizar un acta notarial que dé constancia de la existencia de la información objeto de reclamación, lo que refuerza dicha evidencia probatoria.
- En el caso de que el comportamiento sea constitutivo de delito:
    - Denunciar los hechos ante la autoridad competente y esperar a su actuación.

- Requerir expresamente al proveedor el bloqueo de la información anunciando un posible ejercicio posterior de acciones legales.

En todo caso, la Agencia Española de Protección de Datos pone a disposición de los ciudadanos una sede electrónica con la finalidad, entre otras actuaciones, de solicitar la tutela de derechos o plantear una denuncia[18] en relación con sus datos personales.

Imagen de la sede electrónica de la AEPD

2) Denuncia judicial frente a atentados a la reputación

En primer lugar, para ejercer el derecho[19] de rectificar la información difundida por cualquier medio de comunicación social de hechos que aludan al usuario, que considere inexactos y cuya divulgación pueda causarle perjuicio se debe:

[18] Disponible en: http://sedeagpd.gob.es/sede-electronica-web/

La solicitud de tutela de derechos puede ejercerse en las agencias autonómicas de la Comunidad Autónoma de Madrid, País Vasco o Cataluña, en el caso de que los ficheros de datos sean de titularidad pública (de administraciones públicas autonómicas, locales y otras distintas de la del Estado).

- Remitir un escrito de rectificación al director o responsable del medio de comunicación. Este escrito debe ser remitido dentro de los siete días naturales siguientes al de publicación o difusión de la información que se desea rectificar. En este comunicado se debe indicar:
    - Datos de identificación del reclamante.
    - Información que se solicita sea rectificada.
    - Causas que justifican esta rectificación.
- El contenido de la rectificación debe referirse a los hechos de la información que se desea rectificar.
- Emplear un medio, como un burofax, que permita tener constancia de su fecha y de su recepción.
- De manera opcional, proponer un texto de rectificación (su extensión no debe exceder del de la propia información que se pretenda rectificar).

El medio de comunicación social tiene el deber de proceder a la rectificación o denegarla dentro de los tres días siguientes al de la recepción de la petición.

De estimarla, la rectificación se publicará con relevancia semejante a la original, sin comentarios ni apostillas. Cuando la petición no sea atendida en plazo, sea denegada, o no sea atendida correctamente, el usuario puede ejercitar la acción de rectificación dentro de los siete días hábiles siguientes ante el Juez de Primera Instancia del domicilio o ante el del lugar donde radique la dirección del medio de comunicación.

En segundo lugar, se puede ejercer el derecho al resarcimiento por los daños en vía civil[20]. Para defender en sede judicial el derecho y exigir un resarcimiento resulta necesario interponer una demanda en vía civil ante el Juzgado de Primera Instancia del domicilio del demandante[21]. Esta demanda se tramitará conforme a lo previsto para el procedimiento de juicio ordinario[22].

[19] De acuerdo con la Ley Orgánica 2/1984, de 26 de marzo, reguladora del Derecho de Rectificación.

[20] Con independencia del procedimiento general de exigencia de responsabilidad por daños de los artículos 1902 y ss. del Código Civil, la defensa judicial y la exigencia de resarcimiento de los daños causados a los derechos de la personalidad relacionados con la vida privada, se encuentra prevista tanto por 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 como por el artículo 19 de la LOPD que reconoce el derecho a ser indemnizados de quienes sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto por la citada Ley.

[21] Artículos 45 y 52 de la Ley de Enjuiciamiento Civil

[22] Artículo 249.2 de la Ley de Enjuiciamiento Civil

3) Denuncia de posibles delitos informáticos

Las Fuerzas y Cuerpos de Seguridad disponen de unidades policiales especializadas y canales de denuncia a disposición de los usuarios para situaciones de delitos vinculados con la identidad digital:

- La Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía[23] actúa, entre otros supuestos, en los casos de injurias y calumnias, protección al menor y pornografía infantil en el uso de las nuevas tecnologías, seguridad lógica (robo de información, hacking, revelación de secretos, suplantación de identidad).

- La Guardia Civil cuenta con un Grupo de Delitos Telemáticos[24] creada para investigar, dentro de su Unidad Central Operativa, todos aquellos delitos que se cometen a través de Internet.

6.2 RECOMENDACIONES DIRIGIDAS A LOS PODERES PÚBLICOS

Existen distintos problemas cuya solución podría venir determinada por actuaciones de los poderes públicos mediante la acción del Estado-Legislador, o Estado-Regulador, promoviendo una estructura de apoyo y denuncia, fomentando políticas públicas y acciones de divulgación, incluyendo nuevos contenidos en el sistema educativo o estudiando casos de éxito en iniciativas nacionales e internacionales sobre identidad digital y reputación online. Entre otras cabe formular las siguientes recomendaciones:

[23] Disponible en: http://www.policia.es/colabora.php
[24] Más información en: https://www.gdt.guardiacivil.es/webgdt/pinformar.php

1) Desarrollo normativo

En el ordenamiento jurídico existen herramientas útiles para abordar muchos de los riesgos estudiados en esta guía. Sin embargo, resulta necesario completar el marco jurídico existente con iniciativas específicas:

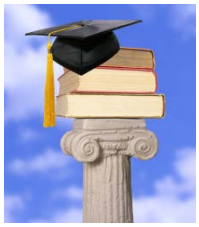
- Llevar a cabo una acción legislativa que defina el significado de los medios de comunicación en Internet y fije pautas de regulación del periodismo ciudadano que incorporen garantías para las personas cuya información aparece en blogs y espacios de Internet equivalentes.

- Regular la repercusión del principio de veracidad sobre las hemerotecas, garantizando que el perfil de una persona responda con veracidad a los hechos. Por ejemplo, recogiendo la libre absolución de quien inicialmente fue imputado o facilitando la visibilidad de las oportunas rectificaciones.

- Consignar en la normativa penal el delito de suplantación de identidad en Internet, y en general la regulación de conductas relacionadas con fenómenos como el grooming o el ciberbullying. Estos fenómenos requieren tanto de una mayor precisión y claridad en la tipificación, como en la persecución de conductas con graves consecuencias sociales.

- Revisar el funcionamiento de algunas instituciones y principios jurídicos, como la publicidad en boletines oficiales de sanciones, indultos y otras informaciones a la luz de los principios de proporcionalidad y mínimo impacto en los derechos de las personas y considerando la operatividad del derecho al olvido.

2) Impulso de recursos educativos, informativos y políticas de innovación



El segundo ámbito estratégico en la actuación de los poderes públicos afecta al sector educativo entendido en sentido amplio, no sólo desde el punto de vista de la formación en sentido estricto sino incluyendo también las políticas de fomento de la investigación y de concienciación social. Para ello:

- Lograr el compromiso de las autoridades educativas para incorporar en los planes de formación nociones sobre vivencia en Internet. Este esfuerzo debería abarcar la formación de:

    - Los futuros maestros y profesores, en sus respectivos planes de estudio.

    - Los profesionales en ejercicio.

- Los estudiantes.
- Los adultos.

- Tutelar en el propio entorno escolar la adquisición de la primera identidad digital por los menores. En dicho ámbito el menor puede realizar de modo organizado y en un ámbito protegido todas y cada una de las acciones que le permiten conformar una identidad en el mundo online.

- Mejorar la efectividad de los canales de denuncia y facilitar su conocimiento y utilización.

- Conseguir una mayor coordinación entre los diferentes agentes que conforman el sistema institucional de respuesta a los diversos atentados al ejercicio de los derechos en Internet. En concreto, puede resultar prometedora la ampliación de los servicios de emergencia al entorno online.

6.3 RECOMENDACIONES DIRIGIDAS A LOS PROVEEDORES DE PLATAFORMAS Y SERVICIOS DE INTERNET BASADOS EN WEB SOCIAL

Los proveedores de servicios se enfrentan al reto de promover un entorno favorable a la identidad digital y a la reputación online a través de distintas acciones que fomenten una cultura de conocimiento y seguridad. Se trata de un compromiso corporativo con la calidad y la confianza de los usuarios en sus servicios. Es recomendable:

- Contar con políticas internas que garanticen que la organización es rigurosa en el cumplimiento de sus obligaciones legales (también llamado *compliance*).

- Disponer de herramientas de diagnóstico que evalúen que las nuevas iniciativas resultan acordes desde un punto de vista ético y en su implementación se garantiza la viabilidad jurídica, como por ejemplo con la implantación de asesorías de impacto sobre la privacidad (*Privacy Impact Assessments*).

- Garantizar una aplicación rigurosa de los principios de protección de datos y en particular los relativos a la información en la recogida de los datos, el consentimiento, la proporcionalidad -entendida en el sentido de mínimo impacto para la privacidad- y la garantía de los derechos ARCO.

- Utilizar recursos técnicos como las instrucciones y etiquetas insertas en páginas web para limitar el barrido de los robots de los buscadores.

- Facilitar herramientas accesibles y usables que permitan un verdadero control por el propio usuario de la información que revela con una gestión consciente de su reputación en Internet.

- Definir códigos éticos de comportamiento recomendado a sus usuarios de modo que al registrarse en el servicio dispongan de pautas de actuación claras.

- Diseñar e implantar acciones de responsabilidad social corporativa que permitan proporcionar "consejo al usuario".

- Desarrollar códigos de conducta internos en la gestión de la identidad corporativa, que sean eficaces y comprometidos con los derechos de los individuos.

- Habilitar canales de denuncia que permitan al individuo alertar sobre situaciones de riesgo en el uso del servicio.

- Colaborar con los poderes públicos y en especial con las Fuerzas y Cuerpos de Seguridad del Estado para la prevención y erradicación de los riesgos asociados a la utilización de identidades digitales por parte de los usuarios.

7 Iniciativas y buenas prácticas en la gestión de la identidad digital

7.1 RECURSOS PARA REFLEXIONAR SOBRE LA IDENTIDAD Y REPUTACIÓN ONLINE (TUSENTIDOCOMUN.COM)

Tusentidocomun.com[25] es una campaña de la Oficina de Seguridad del Internauta (OSI) de INTECO que trata de concienciar al usuario de Internet sobre las amenazas de seguridad y privacidad que puede encontrar en su vivencia online. El enfoque de la campaña está en la importancia de reflexionar sobre los principales comportamientos de los navegantes que pueden desembocar en experiencias no deseadas para su identidad y reputación online.

Para ello, la página web dispone de diversos recursos amenos y prácticos, como por ejemplo:

- Web cómic con historias que ejemplifican situaciones no deseadas en Internet.
- Sello "Yo lo tengo", que permite descargar un sello de navegación responsable y respetuosa para los sitios web personales.
- *Sentidómetro*, o juego online para evaluar si el usuario se comporta adecuadamente en la Red.

7.2 PERFILES DE IDENTIDAD DIFERENCIADOS EN EL SMARTPHONE (DUAL PERSONA)

Una de las mejores prácticas para la protección de la identidad digital consiste en la separación de la actuación personal y profesional. En este sentido, ***Dual persona***[26] es una iniciativa conjunta de Telefónica y VMware para dispositivos smartphone Android, que emplea técnicas de virtualización móvil y cloud computing al perfil profesional, consiguiendo separar completamente el entorno corporativo del personal, en cuanto al uso del terminal.

Los proveedores destacan que la experiencia para el usuario es similar a la tenida con un smartphone convencional con un solo perfil. De forma muy intuitiva, al utilizar una aplicación, el individuo puede pasar de un perfil a otro con un simple click, y recibir las notificaciones laborales y personales en cada perfil de forma independiente.

Esta iniciativa permite al usuario disponer de un control total sobre ambos perfiles, a la vez que incrementa la seguridad de los datos y documentos de trabajo consultados en el terminal, que permanecen a salvo en el perfil profesional en la nube.

[25] Más información: http://www.tusentidocomun.com/

[26] Más información: http://comunidad.movistar.es/t5/Blog-Android/MWC-Telef%C3%B3nica-lanzar%C3%A1-el-servicio-Dual-Persona-para-smartphones/ba-p/491419

Este sistema también es ventajoso para la empresa, puesto que en caso de pérdida o robo del dispositivo, o cuando el usuario abandone la organización, mantendrá a salvo la seguridad de la información corporativa.

7.3 CONSEJOS PARA AYUDAR A LOS MENORES A PUBLICAR DE FORMA RESPONSABLE (CUIDATUIMAGENONLINE.COM)

Cuidatuimagenonline.com[27] es una iniciativa que ofrece 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.

Esta iniciativa de Pantallas Amigas está promovida por un conjunto de instituciones y organizaciones de España y de distintos países iberoamericanos, contando con el apoyo de la OEI (Organización de Estados Iberoamericanos) y la RIATE (Red Iberoamericana de TIC y Educación). Destaca la participación del proyecto español Chaval.es.

Cuidatuimagenonline.com trata sobre el uso de los datos personales, las redes sociales, la precaución con el uso de la imagen, el *sexting* o el uso de la webcam. Tiene el objetivo de sensibilizar y formar de manera lúdica mediante recursos educativos online a los menores entre 11 y 15 años sobre aspectos relacionados con la privacidad y el uso seguro de Internet.

7.4 HERRAMIENTA PARA GESTIONAR LA INFORMACIÓN RECOPILADA POR SERVICIOS WEB (DO NOT TRACK)

"Do not track header" es un plugin que el usuario instala a modo de complemento en su navegador y que, una vez activado, permite la navegación anónima, o lo que es lo mismo, permite obviar la recopilación de información del usuario. A su vez, el propietario del sitio web que recopila dicha información tiene que insertar un código especial en su web.

La herramienta permite tres configuraciones distintas:

1. *Opt out:* el usuario impide cualquier recopilación (máximo nivel de privacidad).
2. *Opt in:* el usuario permite el registro de su actividad en los sitios web.
3. *Null:* el usuario no haya expresado ninguna preferencia, en cuyo caso el sistema anula automáticamente el envío de datos.

La herramienta está disponible para Mozilla, Microsoft Internet Explorer, Safari y Opera.

[27] Disponible en: http://www.cuidatuimagenonline.com/

8. Bibliografía

- ALEJANDRA DE LAMA AYMÁ (2006): *La protección de los derechos de la personalidad del menor de edad.* Tirant lo Blanch. Valencia.
- ANITA L ALLEN. (2008): *Dredging up the Past: Lifelogging, Memory, and Surveillance,* en The University of Chicago Law Review, Vol. 75. http://lawreview.uchicago.edu/issues/archive/v75/75_1/index.html
- ANTONIO FUME*RO, GENÍS ROCA y JESÚS ENCINAR* (2007): *Web 2.0. Fundación Orange* España. http://fundacionorange.es/areas/25_publicaciones/publi_253_11.asp
- ARTEMI RALLO y RICARD MARTÍNEZ (coord.) (2010): *Derecho y redes sociales.* Civitas, Cizur Menor.
- COMISIÓN EUROPEA (2011): *Safer Social Networking Principles for the EU.* http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip_2011/index_en.htm
- CONSEJO DE LA UNIÓN EUROPEA (2011): *Conclusiones del Consejo sobre la protección de los niños en el mundo digital (2011/C 372/04)* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:372:0015:0018:ES:PDF
- DOLORS REIG (2012): *Identidades digitales: límites poco claros.* Cuadernos de Pedagogía. Nº 418 Monográfico http://www.cuadernosdepedagogia.com/ver_pdf.asp?idArt=15088
- EU KIDS ONLINE. *Conference papers. Parallel paper sessions, EU Kids Online Conference* http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Conference%202011/Conference.aspx
- GRUPO DE TRABAJO DEL ARTÍCULO 29*. Dictámenes 2/2009, 5/2009 y 2/2010* *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_es.pdf* *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf
- INTECO (2011): *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles*, 2º cuatrimestre 2011 (16ª Oleada) http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_hogares_2C2011
- INTECO (2012): *Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles*, 3º cuatrimestre 2011 (17ª Oleada)

- INTECO–AEPD (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.* http://www.inteco.es/Seguridad/Observatorio/Estudios/est_red_sociales_es

- JULIO ALONSO. *Identidad y reputación digital*. Evoca. *Cuadernos de comunicación*. http://www.evocaimagen.com/cuadernos/cuadernos5.pdf

- KIERON O'HARA, MISCHA M. TUFFIELD y NIGEL SHADBOLT (2008)*: Lifelogging: Privacy and Empowerment with Memories for Life,* en Identity in the Information Society, Volume 1, Number 1, December. http://www.springerlink.com/content/r273l7321v8h85t7/fulltext.pdf?MUD=MP

- MICROSOFT (2012): *Online Profile & Reputation Perceptions Study. Online Repu*tation Management Survey.

- MÓNICA ARENAS (2010): *El consentimiento en las redes sociales on line,* en Derecho y redes sociales*.* Civitas, Cizur Menor.

- M. RUNDLE y P. TREVITHICK (2008): *At a crossroads: 'Personhood' and digital identity in the information society,* STI Working Paper 2007/7. Directorate for Science, Technology and Industry. OECD.

- ÓSCAR DEL SANTO (2011): *Reputación Online para Tod@s: 10 lecciones desde la trinchera sobre tu activo más importante.* http://www.oscardelsanto.com/reputacion-online-para-tods/

- PEW RESEARCH CENTER'S INTERNET & AMERICAN LIFE PROJECT (2012): *Privacy management on social media sites*. http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx

- RICARD MARTÍNEZ (2010): *Protección de datos y redes sociales: un cambio de paradigma,* en Derecho y redes sociales. Civitas, Cizur Menor.

- RICARD MARTÍNEZ (2009): *El derecho fundamental a la protección de datos: perspectivas", en Internet, Derecho y Política. Las transformaciones del derecho y la Política en 15 artículos.* Editorial UOC, Barcelona

- VIKTOR MAYER-SCHONBERGER (2009): *Delete: The Virtue of Forgetting in the Digital Age. Princeton University Press, New Jersey.*

Síguenos a través de:

Web

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación