Identidad y reputación digital
Visión española de un fenómeno global

Francisco José Santamaría Ramos

Foto: construcción de la Torre Emblemática de la U. de Manizales

Resumen

Objetivo: analizar el concepto de identidad digital causada por la traslación de las relaciones sociales al entorno digital. La existencia paralela entre la vida física y la vida virtual genera nuevos conceptos y nuevas actitudes y competencias y hace que las personas físicas y jurídicas deban producir lo que hoy se conoce como identidad digital, que deriva en la reputación digital. *Metodología*: artículo teórico de análisis documental y de la observación de la práctica virtual. *Resultados*: La traslación de la realidad a la virtualidad no es pacífica pues lleva asociadas desventajas que se traducen en que la exposición de la identidad digital pone en riesgo la identidad como la reputación digitales. Sin embargo, los riesgos varían entre una persona física y una persona jurídica. El problema es cuáles son esos riesgos y cuál el marco regulatorio español al respecto. *Conclusiones*: Se ofrecen algunos consejos para poder gestionar adecuadamente la identidad digital.

Palabras Clave: Identidad digital, reputación digital, riesgos digitales, ciberespacio.

Ambiente Jurídico

Centro de Investigaciones Sociojurídicas

Identidad y reputación digital
Visión española de un fenómeno global

Identity and digital reputation
Spanish vision of a global phenomenon

Identidade e reputação digital
visão espanhola de um fenômeno global

Recibido el 2 de febrero de 2015 - aprobado el 28 de febrero de 2015

Francisco José Santamaría Ramos[1]

[1] Profesor de Informática Jurídica (Real Centro Universitario Escorial María Cristina. Centro Adscrito a la Universidad Complutense de Madrid).

santamaria_fj@hotmail.com

Abstract

Objective: To analyze the concept of digital identity caused by the translation of social relations in the digital environment. The parallel existence between physical life and virtual life generates new concepts and new attitudes and skills and makes physical and legal persons should produce what is now known as digital identity, resulting in the digital reputation. *Methodology*: theoretical paper document analysis and observation of virtual practice. *Results*: The translation of reality to virtuality is not peaceful because it leads associated disadvantages that result in the exposure of digital identity threatens the identity and digital reputation. However, the risks vary between a natural person and a legal person. The problem is what those risks and what the regulatory framework in this regard are Spanish. *Conclusions*: some tips to properly manage digital identities are available.

Key words: digital identity, digital reputation, digital risks, cyberspace.

Resumo

Objetivo: analisar o conceito de identidade digital causada pela translação das relações sociais ao entorno digital. A existência paralela entre a vida física e a vida virtual gera novos conceitos e novas atitudes e competências e faz que as pessoas físicas e jurídicas devam produzir o que hoje se conhece como identidade digital, que deriva na reputação digital. *Metodologia*: artigo teórico de análise documental e da observação da prática virtual. *Resultados*: A translação da realidade à virtualidade não é pacífica, pois está associada a desvantagens que se traduzem em que a exposição da identidade digital põe em risco a identidade como a reputação digital. Porém, os riscos variam entre uma pessoa física e uma pessoa jurídica. O problema é quais são esses riscos e qual é marco regulatório espanhol ao respeito. *Conclusões*: Oferecem se alguns conselhos para puder administrar adequadamente a identidade digital.

Palavras Chave: Identidade digital, reputação digital, riscos digitais, ciberespaço.

Introducción

Debemos a Timothy John Berners-Lee que hoy en día podamos navegar a través de Internet, la autopista de la información. Berners-Lee ideó las líneas maestras sobre las cuales se sustenta la navegación web, gracias a su protocolo HTTP (Hypertext Transfer Protocol) que hace posible la visualización de las páginas web, y al lenguaje HTML (Hypertext Markup Language) con el que se programan esas páginas; estos nos permiten viajar por internet tal como lo conocemos hoy.

Al principio de la era de Internet, las páginas web eran sitios en los que la información sólo corría de forma unidireccional; es decir que tanto los contenidos como la información eran desarrollados por los administradores de las páginas web, llamados webmasters, quienes decidían, en primera y última instancia, cómo serían el contenido y la información que se mostraría en cada página web, de modo que solo existían dos roles en Internet: los webmaster y los usuarios o consumidores de la información que contenía la red.

Con el tiempo, Internet evoluciona y, como consecuencia, los roles en Internet, también lo hicieron. A través de algunos avances tecnológicos, la dictadura de los webmaster empieza a desaparecer; surgen nuevos servicios, como los foros y los chats en la web que permiten que los usuarios (hasta ahora, meros consumidores) empiecen a generar contenidos que pueden compartir entre ellos. Ya no es necesario ser un especialista en informática o dominar el lenguaje HTML para poder publicar información en Internet. Los usuarios comienzan a tomar el control de la red de redes, haciendo pivotar su eje hacia un sistema mucho más comunicativo e interactivo que promulga el intercambio de ideas y conocimiento.

En la última década del siglo XX y principios de siglo XXI asistimos a una auténtica revolución. La dictadura de los webmaster ha sido quebrada, la revolución de los internautas ha generado un cambio actitudinal y surge un nuevo concepto, "Web 2.0", acuñado por Tim O´Reilly, quien lo basa en siete principios fundamentales que explica durante una conferencia en 2004 (Velich, Huel, Bastidas, & Fernández, 2010)[1].

1 Los siete principios fundamentales de la Web 2.0 pueden consultarse en el siguiente enlace: http://web20tp.blogspot.com.es/2010/06/siete-principios-constitutivos-de-las.html

Cabe tener en cuenta que el concepto Web 2.0 no nace como fruto de los cambios tecnológicos, sino que surge precisamente del cambio de actitud de los propios usuarios de la red de redes. Las demandas de mayor protagonismo de éstos propician una nueva forma de entender la red, una "nueva filosofía" si se quiere, que convierte los perfiles de los internautas en un único perfil con capacidad de consumidor y generador de contenidos. Los usuarios quieren formar parte activa de la generación de contenidos en Internet, desean que la información sea accesible de un modo rápido y fiable y, además, demandan un Internet colaborativo, organizado por comunidades de usuarios con ideas afines a las suyas.

La Web 2.0 se nutre de las grandes posibilidades que nos ofrecen los diferentes servicios accesibles hoy en día a través de la red de redes. Los blog, las wikis, las redes sociales, la sindicación de contenidos y un largo etcétera han sido, también, motores de cambio que han posibilitado que Internet sea un nuevo canal comunicativo, totalmente globalizado y que en la actualidad sea más utilizado en los países desarrollados, que los medios de comunicación clásicos: televisión, prensa y radio.

Más aún, la presente revolución comunicativa también ha generado una traslación de nuestras relaciones sociales al ambiente digital, a Internet. Hemos dispuesto retazos de nuestra personalidad, a veces más de los necesarios, en Internet. Hoy en día es tan importante establecer relaciones sociales en el mundo digital como lo es en el físico.

Esta existencia paralela genera nuevos conceptos así como nuevas actitudes y competencias pero, en el tema que nos compete, lo fundamental reside en reseñar que las personas[2], debido a la revelación digital de ciertos aspectos de nuestra personalidad, que pueden contener datos de nuestra intimidad, de donde se genera lo que hoy en día se conoce como identidad digital.

Como definición de identidad digital usaremos la del INTECO (Instituto Nacional de Tecnologías de la Comunicación): "conjunto de la información sobre un individuo o una organización expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital" (INTECO, 2012a, pág. 5).

2 En este sentido es importante entender que el concepto "persona" puede referirse tanto a las personas físicas como a las personas jurídicas.

Obviamente, hablar identidad digital deriva en que otros conceptos pasen a extenderse al mundo digital, como el da la reputación, que para este caso se basa en la opinión o consideración social que otros internautas tengan de una persona u organización, a partir de la vivencia online.

Para aclarar los conceptos, revisemos la explicación del abogado Julio Alonso, experto en contenidos para Internet:

La identidad es lo que yo soy o pretendo ser o creo que soy. La reputación es la opinión que otros tienen de mí. Se forma en base a lo que yo hago y lo que yo digo, pero también a lo que otros perciben de mis actos o palabras, a cómo lo interpretan y a cómo lo transmiten a terceros (Alonso, 2011, pág. 6).

Sin embargo, esta traslación de nuestra reputación al ambiente digital no es pacífica y, al igual que lleva asociadas ventajas, también implica desventajas que se traducen en que al exponer nuestra reputación digital y, por lo tanto, nuestra identidad digital, existen riesgos o amenazas como, suplantación de identidad, violaciones a la intimidad o al derecho a la protección de datos de carácter personal, difamaciones, etc.

Hemos de tener en cuenta, tal y como señala Julio Alonso (2011), que Internet es un mecanismo extraordinariamente eficiente de comunicación humana; multiplica nuestra capacidad de establecer relaciones; nos libera de los límites que introducen las distancias geográficas e incluso, de muchos prejuicios, al permitirnos comunicarnos y relacionarnos con personas que viven a miles de kilómetros de distancia y que a priori no parecen tener nada en común con nosotros. Todo esto tiene un muy fuerte impacto en los procesos de creación de identidad y reputación.

Además del riesgo por la exposición de nuestra identidad y reputación en un medio inseguro como Internet, también hay que considerar que, las reglas de generación de identidad y reputación no son las mismas que en el mundo físico o, al menos, no son exactamente iguales debido fundamentalmente a varios motivos (Alonso, 2011):

- Permanencia de la información: Como regla general, lo que se publica en Internet suele permanecer sobre todo porque el usuario habitualmente no controla el servicio en el que está dejando la información y porque no es posible evitar la replicación de contenidos.

- Visibilidad o facilidad para localizar los contenidos: Cualquier contenido, en Internet, es susceptible de ser localizado, indexado, copiado y enlazado.
- Credibilidad de las fuentes de información: Internet supone riqueza informativa dado que es posible localizar muchos más puntos de información sobre cualquier cuestión. No obstante, los conflictos de interés en la generación de reputación se hacen más evidentes y los individuos anónimos pero con reputación y, sobre todo, independencia, tienen más credibilidad para opinar. Por tanto debemos ser conscientes de una cuestión clave: la construcción de la reputación es cada vez más colaborativa y depende cada vez más de la opinión de terceros.
- Micro-expertos: Los aficionados han encontrado en la red de redes y, sobre todo, en la "filosofía 2.0" una vía para poder compartir su experiencia y sus conocimientos; esto los convierte en fuentes de información de primer nivel y, en tanto en cuanto se mantienen alejados de los potenciales conflictos de interés, se convierten en importantes influenciadores.
- Velocidad: Internet ha mejorado sus tiempos de respuesta y hoy la información es prácticamente compartida en tiempo real.

Por tanto, en este escenario, hay que tener en cuenta que los riesgos no son los mismos en la identidad y la reputación digital y que además, varían en función de si se trata de una persona física o de una persona jurídica. En todo caso, para ambas es aplicable lo que establece Ruth Gamero (2009) en su libro La configuración de la identidad digital:

La construcción de una identidad requiere esfuerzo y tiempo, y una especial sensibilidad para entender que nuestros actos tienen repercusión en los demás. No es sencillo crear una imagen reconocida por el otro con la que, además, estemos a gusto y que nos pueda acompañar muchos años, crecer con nosotros (pág. 1) .

Como ya hemos dicho anteriormente, la identidad digital personal supone no sólo la visibilidad en Internet de una persona física sino también su reputación e intimidad dentro de la red de redes; adicionalmente, tal y como sostienen Aiana Giones y Marta Serrat (2010), actualmente en el campo del marketing la identidad digital está en auge y se conoce como identidad digital corporativa.

Situando con claridad el escenario, a lo largo de las próximas líneas trataremos de arrojar algo de luz sobre cuáles son los riesgos a los que podemos vernos expuestos, cuál es el marco regulatorio español en este sentido y presentaremos algunos consejos para poder gestionar, de una forma adecuada, nuestra identidad digital.

Personas físicas

La identidad digital

La Organización para la Cooperación y el Desarrollo Económicos (OCDE), que tiene como finalidad principal promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo, nos ofrece un documento sobre cuáles son las características de la identidad digital, titulado, At a Crossroads: "Personhood" and digital identity in the information society (Rundle, y otros, 2008).

En este sentido, la OCDE establece que la identidad digital tiene 8 características fundamentales:

1. Es social: Cuando se proyecta en Internet, los internautas caracterizan y reconocen de forma efectiva a su poseedor incluso aunque no se haya producido una verificación presencial de la identidad.
2. Es subjetiva: Se basa en la experiencia que los diferentes internautas construyen y que, por tanto, les permite reconocerse.
3. Es valiosa: Se genera una ingente cantidad de información que puede ser empleada para establecer relaciones personalizadas así como para tomar decisiones en dichas relaciones, con lo que se establece un mayor grado de confianza.
4. Es referencial: La identidad digital se basa en una referencia a una determinada persona u objeto.
5. Es compuesta: La información puede ser suministrada, bien de forma voluntaria por el propio sujeto o bien suministrada y construida por terceros, sin la participación del mismo.
6. Genera consecuencias: La divulgación puede generar efectos e incluso, la no divulgación es la que puede generar dichos efectos.

7. Es dinámica: Se modifica constantemente. Es un flujo de información en constante movimiento. La identidad digital no es, en absoluto, estática.
8. Es contextual: Su divulgación puede generar un impacto negativo si se utiliza en un contexto erróneo o, sencillamente, ser irrelevante. En muchas ocasiones, mantener las identidades segregadas permite obtener una mayor autonomía.

La reputación on-line

Se basa en la opinión o consideración que se tiene de algo o de alguien, o en el prestigio en que se estime a alguien o algo. En general, el ser humano aspira a ser valorado en su entorno y a tener una buena reputación. Sin embargo, la reputación on-line tiene una serie de diferencias que la desmarcan del concepto de reputación más clásico o, si se prefiere, físico:

- La reputación online es acumulativa en el tiempo. Digamos que Internet no permite el olvido fácilmente ya que siempre, hagamos lo que hagamos en la red de redes, dejamos un rastro o una huella, difícil de borrar. Nuestra reputación en el ámbito digital se genera a través de una gran cantidad de datos de carácter personal que pueden ser localizados con extrema facilidad incluso sin que seamos conscientes de dicha situación.
- Alto grado de alcance y repercusión. Cualquier internauta se encuentra capacitado para propagar información y opiniones a través de Internet que a su vez pueden localizarse fácilmente y, peor aún, difundirse rápidamente a través de la red.

Ahora entremos en una cuestión de vital importancia: ¿Cómo se construye la reputación digital?

Básicamente puede construirse a través de 3 factores:

- Acciones desarrolladas por el propio titular: Trasladando nuestras vivencias y nuestra información personal al entorno digital.
- Acciones desarrolladas por terceros: Aquella información sobre la reputación del titular que se encuentra disponible en el entorno digital y que ha sido producida y difundida por terceros.

- Acciones desarrolladas en el entorno del titular: Las relaciones desarrolladas en Internet también agregan datos y, por lo tanto, afectan la construcción de la reputación de los implicados en dichas relaciones.

Riesgos

Aunque los riesgos relacionados con la identidad digital y la reputación on-line son variados, todos reúnen una característica común; son riesgos que podríamos denominar entrelazados, es decir, el más mínimo riesgo puede verse acrecentado, de forma exponencial, por sus derivaciones y colateralidades asociadas al resto de impactos. Por lo tanto, es esencial minimizar cualquiera de los impactos que exponemos de manera detallada en el siguiente apartado.

Suplantación de nuestra identidad digital

Como su nombre lo indica, sucede cuando una persona (generalmente malintencionada), se apropia de nuestra identidad digital y actúa en nuestro nombre.

La suplantación puede tener diversas caras:

- Registro de perfiles falsos en los que no se utiliza información personal de quien se pretende suplantar. Un claro ejemplo son los perfiles caricaturizados de personajes públicos o relevantes.
- Registro de perfiles falsos utilizando información personal de quien se pretende suplantar.
- Acceso no autorizado a perfiles. En este caso, los atacantes pretenden, en primer lugar, perjudicar la imagen y la reputación on-line de la persona, alterando datos del titular del perfil. Generalmente, este tipo de intrusiones tienen como finalidad secundaria, menoscabar la economía de la persona suplantada.

Riesgos en la Privacidad

Se producen gracias a la eclosión y masificación de las redes sociales. Normalmente publicamos una gran cantidad de información en la red sin ser plenamente conscientes de que en el momento en el que la publicamos perdemos el control sobre sus posibles usos y difusión. Los atacantes aprove-

chan esta situación para capturar nuestra información personal y utilizarla inadecuadamente.

Este tipo de riesgos se caracterizan porque impiden a las personas ejercitar un correcto control sobre sus datos personales.

Riesgos sobre la reputación on-line

Estos son aquellos riesgos que pueden afectar al prestigio u opinión que una persona ha adquirido en Internet. En comparación con el mundo físico, suponen un riesgo mucho mayor porque en Internet los contenidos se difunden con una mayor rapidez.

Pueden desglosarse de la siguiente manera:

- Publicaciones que exceden la libertad de información porque violan la intimidad de las personas, incluso la de aquellas que sean famosas o relevantes dentro de la vida pública.
- Publicaciones falsas, injurias y calumnias. Este tipo de situaciones constituyen una flagrante vulneración del honor de las personas.
- Descontextualización de la información: En algunas ocasiones, y a pesar de las grandes ventajas que nos aportan los buscadores, es posible localizar información del pasado, relativa a las personas, y que sacadas de contexto pueden perjudicar seriamente, tanto al titular de dicha información como a sus familiares y allegados. Esta situación ha posibilitado que hoy en día se hable de un nuevo derecho relacionado a la protección de datos de carácter personal: el derecho al olvido.

Vulneración de los derechos sobre propiedad intelectual

Las personas, generalmente, tienen la percepción de que todo lo que está en Internet se puede utilizar libremente sin que dicha información tenga, forzosamente, que ser veraz. En muchas ocasiones, las personas vulneran los derechos de otras al relacionarlos con contenidos de terceras personas (imágenes, audios, contenidos audiovisuales, etc.).

Dicha situación no sólo supone una vulneración de los derechos de propiedad intelectual sino que también puede ocasionar menoscabo de la reputación y de la identidad digital de su autor.

Normativa

La legislación no es extraña a los cambios surgidos a raíz de la evolución de las Tecnologías de la Información y las Comunicaciones y, aunque la Constitución Española de 1978 sea fruto de su tiempo y no contemple expresamente un derecho fundamental a nuestra identidad y reputación on-line, sí que contiene articulado suficiente para que podamos asociar estos nuevos conceptos a las debidas protecciones jurídicas que nos ofrece el Derecho español.

A continuación vamos a desglosar de una forma somera los diferentes derechos relacionados con nuestra identidad digital y nuestra reputación on-line.

Derecho al honor, a la intimidad personal y familiar y a la propia imagen

Consagrado como un derecho fundamental, protege cierta esfera de nuestra personalidad, de carácter subjetivo y que se traduce en proteger a las personas para que no sean víctimas de determinadas agresiones:

- Honor: Es el sentido del aprecio o estima del que gozamos las personas en un círculo social determinado. Protege a las personas de la exposición de noticias u opiniones, infundadas, que puedan desmerecer o menoscabar dicho aprecio o estima.
- Intimidad: Se trata de cierto espacio o esfera, de carácter personal, sobre la que tenemos la libertad tanto de excluir a terceras personas como de impedir intromisiones en ésta.
- Propia imagen: Se trata de los atributos característicos, propios e inmediatos de las personas, como la voz, la imagen física o el nombre. Las personas gozamos de un poder de disposición respecto al uso que cualquier tercero quiera realizar de estos atributos, quien requerirá nuestro consentimiento para ello.

A pesar de lo dicho, los derechos reflejados anteriormente no son absolutos. Al contrario, disponen de su propia némesis que se traduce en dos derechos fundamentales de especial relevancia y que, en algunas ocasiones pueden chocar con los derechos arriba mencionados. Nos referimos a los derechos a la información y a la libertad de expresión que se popularizado con el auge de las Tecnologías de la Información y las Comunicaciones y la "filosofía" Web 2.0.

- La libertad de información faculta u otorga el derecho a las personas a publicar noticias, siempre que éstas sean veraces; lo que supone que previamente deben haber sido verificadas y contrastadas, así como disponer de cierta relevancia pública, es decir, que la noticia debe ser socialmente importante.
- La libertad de expresión faculta u otorga a las personas poder para publicar sus pensamientos, opiniones o ideas, siempre teniendo presente que debe expresarse que se trata de una valoración subjetiva de la realidad.

Ambos derechos deben ser utilizados prudentemente puesto que un inadecuado uso puede acarrear violaciones que nos exijan posteriores responsabilidades, por ejemplo la petición de indemnizaciones resultantes de los perjuicios causados al derecho al honor, a la propia imagen o a la intimidad personal y familiar de las personas afectadas.

Protección de datos personalles[3]

Consagrado como derecho fundamental por el Tribunal Constitucional, a través de la sentencia 292 del 30 de noviembre de 2000, faculta a las personas a controlar sus datos de carácter personal así como a disponer de un poder de control y decisión sobre los mismos (Sentencia 292/2000). La legislación española otorga a las personas una serie de derechos sobre la protección de datos de carácter personal:

- Derecho de acceso: Permite que las personas se dirijan al responsable del fichero o del tratamiento para solicitar y obtener, de forma gratuita, información sobre los datos de carácter personal que obran en poder de dicho responsable así como el origen de los mismos y

3 Aunque la normativa en materia de protección de datos de carácter personal es mucho más compleja y extensa, para la materia que nos compromete no es necesario indicar de todas las obligaciones que impone. No obstante se reflejan, en este punto, algunas cuestiones de especial relevancia:

- Deber de información: Que obliga al responsable del fichero o tratamiento a informar a las personas de la incorporación de sus datos personales a un fichero así como de la identidad y dirección del responsable, de la finalidad del fichero, de los destinatarios de la información y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- Cuando un responsable del fichero o tratamiento quiera tratar datos de carácter personal, deberá solicitar el consentimiento de las personas, previamente al tratamiento de sus datos personales.

las posibles cesiones o comunicaciones que de los mismos se hayan realizado a terceros.

- Derecho de rectificación: Establece el derecho de las personas a solicitar al responsable del fichero o del tratamiento que se rectifiquen los datos personales cuando éstos sean inexactos o incompletos.
- Derecho de cancelación: Otorga a las personas la facultad de dirigirse al responsable del fichero o del tratamiento para solicitar la cancelación de sus datos de carácter personal.
- Derecho de oposición: Facultad que tienen las personas para oponerse a que sus datos sean tratados con una finalidad comercial o de marketing.

Derecho al olvido

En los últimos tiempos, este derecho ha cobrado una relevancia mediática especialmente importante. Se configura como la facultad que disponen las personas para que una determinada información sea eliminada del contexto de Internet y, particularmente, para que determinada información, de carácter personal, no pueda ser indexada por los buscadores (Google, Yahoo, etc.).

Herencia digital

Tanto Internet como la Web 2.0 han supuesto un giro radical en la forma de concebir nuestra identidad y nuestra reputación, durante el desarrollo de nuestra vida, al momento de nuestro fallecimiento y posterior a éste.

Internet puede guardar determinada información personal aunque la persona ya haya fallecido e incluso, puede generarse nueva información. En este sentido, algunos proveedores de servicios en Internet, generalmente las redes sociales, tienen en cuenta este asunto y articulan determinados mecanismos para que las personas ligadas estrechamente al fallecido puedan cerrar su respectivo perfil; también, algunos proveedores, como Facebook, permiten mantener un perfil "conmemorativo".

Responsabilidad de los prestadores de servicios de la Sociedad de la Información

Los servicios que se prestan a través de Internet y que permitieron el auge de los servicios Web 2.0 son administrados, como regla general, por terceros.

En España, la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (Ley 34/2002, 2002), comúnmente denominada LSSI, fija un régimen de responsabilidad para los prestadores de servicios de la Sociedad de la Información.

Dicha responsabilidad puede ser civil, penal y administrativa y, en modo alguno, es absoluta puesto que las conductas de los usuarios de sus servicios pueden suponer una exención de la responsabilidad de éstos:

- El proveedor no se encuentra obligado a supervisar o monitorizar los mensajes que circulan a través de su servicio así como los datos o contenidos alojados en sus sistemas o equipos informáticos, ni de los hiperenlaces incluidos por los usuarios.
- El proveedor no responde por 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.

Algunos consejos prácticos

La condición primera y más importantes es que los usuarios debemos ser plenamente conscientes de que somos nosotros mismos quienes debemos velar por cuidar nuestra identidad digital y nuestra reputación on-line. Nosotros somos los principales responsables de cuidar los perfiles que utilizamos a través de la red de redes.

Dicho esto, las personas deberemos tener en cuenta los siguientes consejos prácticos para tratar de minimizar los riesgos que podrían sufrir nuestra identidad digital y nuestra reputación on-line:

Creación de perfiles

En relación con la creación de perfiles, es necesario tener en cuenta las siguientes recomendaciones:

- Antes de crear un perfil debemos pensar si realmente nos va a ser útil y sopesar dicha utilidad en relación con la seguridad de nuestros datos de carácter personal. ¿Realmente es útil publicar nuestra información en este servicio? Esta debe ser la primera pregunta.

- Antes de crear el perfil debemos verificar las políticas de protección de datos de carácter personal del servicio así como las posibles responsabilidades tanto del usuario como del prestador del servicio.
- Para minimizar el riesgo que nuestra imagen sea difundida de forma inadecuada, podemos parcelar nuestra identidad en la red a través de diversos perfiles tanto personales como profesionales.

Seguridad y privacidad de los perfiles

Antes de publicar cualquier tipo de contenido es conveniente aprender el funcionamiento y las opciones de configuración relativas a nuestra información, de forma que seamos nosotros mismos quienes garanticemos, en primer término, el control de nuestra información y de las relaciones que creamos a través de dicho perfil.

En este sentido es altamente recomendable:

- Configurar la seguridad y privacidad de nuestra información dentro de nuestro perfil.
- Sopesar todo aquello que tengamos intención de publicar con la finalidad de no perder el control de la información que puede difundirse a través de Internet.
- Utilizar, en exclusiva, aquellas aplicaciones que puedan utilizarse dentro de nuestro perfil así como limitar las publicaciones que dichas publicaciones puedan realizar en nuestro perfil.
- Siempre que terminemos de realizar operaciones en nuestro perfil es muy importante cerrar la sesión para evitar que terceros accedan a ésta.
- Conciencia y actitud de respeto dentro de Internet

Es necesario tener en cuenta que:

- Nunca debemos informa u opinar sobre un asunto si no estamos totalmente seguros de lo que vamos a decir y, en todo caso, usando un tono respetuoso y tolerante.
- Cuando se utilice información relativa a terceras personas es importante pedir permiso al titular de dicha información y evitar utilizar los mecanismos tendentes al etiquetado de dicha información.
- Cumplir con los términos y condiciones del servicio al cual accedamos.

Hábitos durante la navegación

Es necesario tener en cuenta:

- Utilizar antivirus y otros programas de seguridad y mantenerlos actualizados siempre que nuestros equipos y sistemas informáticos utilicen Internet.
- En la medida de lo posible, se debe evitar la instalación en nuestros equipos y sistemas informáticos de cookies[4] o cualquier otro dispositivo de trazabilidad. En caso de no poder evitarlo, por pedir prestaciones o el empleo correcto del servicio en línea, ser plenamente conscientes del uso y utilidad que para el proveedor del servicio tienen dichas cookies.
- Desactivar la concesión de permisos a los servicios de búsqueda de información y publicidad o, en su caso, revisar dichos sistemas.

Mantenimiento de la identidad

En este sentido, es necesario tomar dos medidas estrictamente necesarias:

Por un lado, hay que verificar nuestras identidades digitales en Internet, como medio para prevenir alteraciones o usos indebidos de nuestra identidad y, en caso de encontrar desaciertos, aplicar las medidas correctoras que sean necesarias para restaurar nuestra identidad digital.

Se recomienda verificar los cambios en las políticas de privacidad de los servicios en los que se encuentren alojadas nuestras identidades digitales. Dichos términos o políticas pueden afectar la información que sobre nosotros, se difunde públicamente y si esto sucede es necesario aplicar nuevas preferencias de privacidad y seguridad para evitar que suceda nuevamente.

Salvaguarda de nuestros derechos a través de los proveedores de servicios

Cuando pensemos que nuestros derechos como usuarios o incluso, los derechos de terceros (ajenos al servicio) se están vulnerando, es necesario utilizar los sistemas de denuncias ofrecidos por los proveedores de servicios.

4 Una cookie es una pequeña información enviada por un sitio web, que se almacena en el propio navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

En este sentido, lo más importante es tener presentes los derechos que nos asisten en materia de protección de datos de carácter personal (acceso, rectificación, cancelación y oposición) y ejercerlos de forma directa ante el proveedor del servicio.

En algunas ocasiones, aunque el proveedor del servicio atienda nuestras peticiones, es posible que la información no desaparezca de los buscadores o de otras páginas web, por lo que, en dichas situaciones, el ejercicio de nuestros derechos, también deberá hacerse frente a dichos terceros.

En este punto es importante recordar que la responsabilidad de los proveedores no nace hasta que poseen un conocimiento efectivo de la situación que está perjudicando a los usuarios y, por tanto, es necesario aplicar el adecuado canal de denuncia, que generalmente está definido en los términos y políticas de uso de la web.

En todo caso, el ejercicio de nuestros derechos puede suponer una pérdida de información y, en este sentido, es altamente recomendable:

- Realizar copias de pantalla de la información que se quiera cancelar o rectificar o, en su caso, de la conducta que se desea perseguir. En dicha copia de pantalla deben constar la dirección de Internet y la fecha en la que se realizó dicha copia. Lo dicho anteriormente, si bien es recomendable, puede tener poco peso probatorio por lo que, muchas veces, lo más práctico es levantar un acta notarial que deje constancia de la información objeto de la reclamación
- Si la acción a perseguir es constitutiva de delito, lo mejor que podemos hacer es denunciar los hechos ante la autoridad competente y requerir al proveedor el bloqueo de la información avisándole expresamente que podrían iniciarse acciones legales.

Reputación y denuncias judiciales

Hablamos de la posibilidad que tenemos las personas o de la potestad que nos concede el derecho, para poder rectificar la información difundida por los medios de comunicación y que aluden a hechos concretos de las personas, quienes consideran que son inexactas y que, además, dañan o merman su reputación y, por tanto, pueden causarle un perjuicio.

En este sentido, más que el mecanismo o procedimiento a través del cual las personas podemos ejercitar la presente acción, lo más importante que se debe tener en cuenta es que una vez la reclamación de la persona llega al medio de comunicación, él mismo tiene el deber de proceder a su estimación o a su denegación, siempre dentro de los 3 días siguientes al de la recepción de dicha solicitud o petición.

En el caso de que la solicitud sea estimada, la rectificación deberá ser publicada (en los mismos términos de revelación que la información original) sin comentarios ni apostillas.

En aquellas situaciones en las que la petición sea denegada o no sea atendida correctamente, la persona que realizó la solicitud aún tiene la oportunidad de ejercitar dicha rectificación dentro de los siguientes 7 días hábiles, ante el Juez de Primera Instancia del domicilio o, en su caso, ante el del lugar donde radique la dirección del medio de comunicación.

Denuncia de delitos

En el caso de que se sospeche o se tengan indicios de que se está cometiendo un delito que atenta contra la identidad digital, lo más efectivo es recurrir a las Fuerzas y Cuerpos de Seguridad del Estado, bien a través de la Brigada de Investigación Tecnológica de la Policía Nacional –BIT, bien a través del Grupo de Delitos telemáticos de la Guardia Civil.

Personas jurídicas

Identidad digital

En la actualidad, no cabe ninguna duda, cualquier entidad, empresa, organización, etc. necesita de la red de redes, de Internet, siquiera como mecanismo de apoyo de sus actividades cuando no, un vehículo en sí mismo para desarrollar sus actividades. Por esta razón el mundo del marketing y la publicidad está pivotando y posicionando todas sus habilidades en desarrollar para las entidades una identidad digital, de carácter corporativo que permita establecer un mecanismo de comunicación sólido y funcional, y un mayor contacto con el público en general, con los clientes activos y potenciales, y con los proveedores.

Hoy en día, las redes sociales se han posicionado como una atractiva solución para la promoción de productos y servicios, dado su bajo costo de mantenimiento y su alta capacidad para llegar a un mayor número de personas, lo cual redunda en una mayor comunicación, fundamentalmente con los clientes activos y los potenciales clientes.

A las entidades y corporaciones ha llegado La Web 2.0 para quedarse. La presencia en Internet es fundamental y ya no sólo se trata de tener una página web estática; el blog, las redes sociales y un largo etcétera son parte importante de la comunicación de las organizaciones.

En este escenario, parece que las publicaciones y cómo se dé a conocer determinada entidad u organización compone lo que podría llamarse su identidad digital corporativa. Peroen España, el Instituto Nacional de Tecnologías de la Comunicación, también conocido como INTECO, previene de una circunstancia especialmente relevante: No es necesario que una entidad se encuentre en Internet para que, en dicho medio, puedan surgir opiniones sobre ella y, por tanto, los contenidos generados por terceros se añaden a la identidad digital de la entidad. En este sentido INTECO establece que:

La identidad digital corporativa, por tanto, puede ser definida como el conjunto de la información sobre una empresa expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha organización en el plano digital (INTECO, 2012a, pág. 5).

Reputación on-line

Por otro lado, en sintonía con la identidad digital corporativa, circula el concepto de reputación corporativa on-line que tiene que ver con el valor de una organización, es decir, la percepción del público sobre dicha entidad u organización y que se traslada al mundo digital a través de la filosofía Web 2.0. En este sentido y de acuerdo con el INTECO, podemos decir que:

La reputación on-line es "la valoración alcanzada por una empresa a través del uso o mal uso de las posibilidades que ofrece Internet" (INTECO, 2012b, pág. 9).

Por tanto, es posible hablar de una gestión de la reputación digital de las organizaciones o dicho de otra forma, las entidades, las organizaciones, hoy en día, tienen que empezar a gestionar, adecuadamente, esa valoración que se tiene sobre ellas en el mundo digital.

Riesgos

Internet es un medio inseguro y ofrece una serie de amenazas que pueden generar impactos negativos en la imagen y en la reputación digital de las entidades u organizaciones, teniendo en cuenta que, además, dicho impacto puede acrecentarse por el efecto multiplicador propio de Internet. A lo largo de las próximas líneas vamos a detallar algunos de estos riesgos.

Suplantación de identidad

Su propio nombre nos indica que consiste en la usurpación del perfil corporativo de la entidad u organización por parte de un tercero malintencionado. Además de la usurpación de un perfil ya creado (al cual se accede sin autorización alguna), también contempla la creación de un perfil y su uso posterior como si se tratase de la propia entidad u organización.

Cabe matizar que la suplantación de la identidad no debe confundirse con la parodia o la creación de un perfil caricaturizado de una organización, práctica cada vez más extendida y que tiene como finalidad el uso de dichos perfiles e incluso páginas con claros tintes críticos y que, mientras no vulneren la normativa, es una práctica totalmente lícita.

Cuestión distinta en la suplantación de identidad y que supone, en el mejor de los casos, un perjuicio o menoscabo en la reputación de la organización y que repercute en sus actividades, productos y servicios en el mundo digital y en el mundo físico y, en el peor de los caos puede suponer incluso el mecanismo para la comisión de actividades delictivas tales como el robo de información, el fraude digital o la extorsión, por citar algunos ejemplos.

En este sentido, se destaca el robo de información de los usuarios de la organización o entidad para la comisión de acciones fraudulentas a través de técnicas como el Phishing[5] o el Pharming[6].

5 Phishing: Técnica en al que el estafador, también conocido como phisher, usurpa la identidad de una organización para que el receptor de una comunicación electrónica, con clara apariencia oficial, facilite determinada información que puede resultar útil al estafador.

6 Pharming: Técnica en la que el estafador modifica los parámetros de resolución de nombres de dominio para generar confusión en el usuario y que éste se dirija, de forma automática, a una página web, fraudulenta, que suplanta a la página web oficial con la finalidad, nuevamente, de obtener información útil para el estafador.

Registro de nombres de dominio

Un dominio o nombre de dominio es el nombre que identifica un sitio web. Los nombres de dominio se encuentran asociados a una dirección IP que no es más que un código que utilizan los equipos informáticos para poder comunicarse entre sí.

Dicho esto, cuando una entidad u organización desea tener presencia en Internet, generalmente, tiende a elegir un nombre de dominio fácilmente reconocible por el público y que suele coincidir bien con su nombre comercial, bien con las marcas de sus productos y servicios.

El riesgo asociado a los nombres de dominio viene determinado cuando terceros, claramente malintencionados, registran uno o varios nombres de dominio que coinciden con el nombre comercial o las marcas de determinada organización o entidad, impidiendo a esta última utilizar dichas denominaciones en sus actividades digitales. Este tipo de actividad se conoce con el nombre de cybersquatting y puede producirse en tres momentos determinados:

- Registro del nombre de dominio anticipándose a la entidad u organización.
- Cuanto la entidad u organización olvida proceder a la renovación del nombre de dominio.
- Cuando surgen nuevas extensiones de dominios de nivel superior como por ejemplo los .soy o .tickets y la organización u entidad no realiza el correspondiente registro del dominio.

Este riesgo suele tener dos finalidades muy claras:

- La extorsión propiamente dicha. Aquí el atacante solicita un rescate a la entidad u organización para transferir a su titularidad el dominio.
- Aprovechar la reputación de la entidad u organización para atraer tráfico o visitantes a una determinada página web que, de forma indirecta, repercute en beneficios generados por la publicidad de dicha página Web.

Asimismo, en algunas ocasiones no es necesario recurrir al registro de nombres de dominio idénticos a los nombres comerciales o marcas de de-

terminada entidad sino que se explotan las confusiones o parecidos (Facebok, Youtuve,…) y que se considera una variante del cybersquatting que se conoce con el nombre de typosquatting.

En ambos casos, el riesgo es evidente, se produce un impacto negativo tanto en la identidad como en la reputación de la entidad u organización que, incluso, puede derivar en un beneficio de carácter económico por parte de quien menoscaba la identidad o la reputación de la organización.

Ataques de denegación de servicio

Este tipo de riesgos se producen a través de un conjunto de técnicas que tienen como finalidad principal inutilizar un servidor y que éste deje de funcionar de manera adecuada. Para ello, como regla general, se suelen utilizar varios equipos informáticos que trabajan de forma coordinada y que acceden a una determinada página web o a alguna de sus funciones, con el fin de colapsar el servidor y conseguir que éste no pueda responder al flujo de solicitudes o peticiones.

El colapso da lugar a un funcionamiento anormal de la página web que deriva en que ésta deja de funcionar y pierde la posibilidad de acceso para los usuarios. Por tanto, la entidad o la organización sufre un claro perjuicio en su identidad y en su reputación digital puesto que proyecta una imagen, a sus usuarios, de evidente vulnerabilidad, lo que suele producir desconfianza.

Robo de información

Quizá uno de los riesgos de mayor gravedad para una entidad u organización, en lo relacionado con su reputación digital, es el robo de información, generalmente de carácter sensible (datos personales) o confidencial y su posterior difusión a través de Internet.

El robo de información suele deberse a tres motivos claramente malintencionados: el lucro u obtención de un beneficio de carácter económico, el espionaje de carácter industrial y el desprestigio de la entidad u organización.

Asimismo, existen dos formas en las que este riesgo se manifiesta:

- Interno: Por error o intención de algún empleado de la entidad.

- Externo: Utilizando diversas técnicas, como la infección a través de malware o ataques del estilo Man in the Middle[7].

Desprestigio a través de publicaciones

La Web 2.0 ha supuesto un giro radical y ha dado el poder a los internautas de ser a la vez consumidores y generadores de contenido. Es precisamente la capacidad para generar contenido la que supone un riesgo para cualquier entidad u organización, independientemente de que la misma se encuentre en la Red o no.

¿Qué sucede cuando un internauta genera críticas o comentarios negativos con respecto a una determinada entidad u organización?

Sin duda alguna el riesgo no está tanto en las críticas de determinados internautas como en una dejadez o falta de actuación oportuna de la organización ante dichas críticas. Corresponde a la entidad u organización realizar una defensa activa de su reputación digital y, en este sentido, debe dar adecuadas respuestas y soluciones a las críticas que reciba de sus internautas.

Cuestión distinta ocurre con aquellos comentarios falsos y que dañan la reputación, ya sea digital o no, de determinada entidad u organización. En este punto, la entidad no sólo debe reaccionar adecuadamente sino que también puede activar aquellos canales que le permita la normativa o la legislación y que son tendientes a proteger el honor y la reputación de la entidad u organización.

Vulneración de la propiedad intelectual

Los derechos de propiedad intelectual se configuran como derechos de doble acción o de doble dimensión ya que no sólo permiten que su titular pueda utilizarlos sino que además impide a terceros su uso, salvo que cuente con la debida autorización del primero.

No obstante Internet, por su propia esencia digital, se convierte en un canal proclive a la copia, la modificación y la reutilización de contenidos que,

[7] Man in the middle: Ataque basado en que el propio atacante se posiciona entre el servidor de la organización y el dispositivo que solicita la conexión al servidor, con la finalidad de leer, modificar o filtrar la información que se está transfiriendo.

en algunas ocasiones, forman parte de la propiedad intelectual e incluso industrial de una determinada entidad u organización. Por tanto, su uso o comercialización, sin la debida autorización, se convierte en un delito contra los derechos de propiedad intelectual o industrial e incluso, en algunos casos, podría suponer hasta un delito de competencia desleal.

Es común que los usuarios de Internet tengan poca conciencia en este sentido y piensen que en Internet es posible realizar este tipo de acciones o actividades sin que por ello se esté vulnerando el derecho de terceros. Pero, tampoco debemos ser inocentes. Muchas veces, tras este tipo de acciones, solemos encontrar a terceros malintencionados o incluso a empleados descontentos.

No obstante, sea por una falsa sensación o por una clara intencionalidad, el daño es el mismo y puede suponer no sólo la comisión de un delito de carácter penal sino también un impacto negativo tanto en la identidad como en la reputación de determinada organización o entidad.

Normativa

La protección que se brinda a la reputación digital es muy similar a la que se brinda a la reputación clásica o, si se prefiere, a la reputación del mundo físico. Dicho esto, es necesario realizar ciertas matizaciones que son de vital trascendencia:

- Impacto: La difusión de la información a través de Internet es rápida y viral y, por tanto, no es comparable, en modo alguno, con la difusión de información a través de los canales tradicionales, de modo que el impacto no puede medirse de igual forma.
- Perdurabilidad: Incluso aunque se actúe de forma cuasi-inmediata es altamente improbable que se consiga retirar de Internet una determinada información y, por tanto, esta puede perdurar en el tiempo. Incluso, aunque consiga retirarse la información, ésta puede perdurar en forma de pantallazos o capturas de pantalla o en descargas realizadas antes de lograr la eliminación de la información.
- Efecto Streisand: Se trata de un fenómeno de Internet en el que un intento de censura u ocultamiento de cierta información fracasa o es incluso contraprodu-cente para el censor, ya que ésta acaba siendo ampliamente divulgada, recibiendo mayor publicidad de la que habría tenido si no se la hubiese pretendido acallar.

Teniendo presentes las matizaciones, cabe resaltar que en España las personas físicas se encuentran amparadas por un derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, tal como lo recoge la Constitución Española.

En este sentido, nuestro Alto Tribunal (Tribunal Constitucional) hace partícipe a las organizaciones o entidades de este derecho al honor o, si se prefiere, a una reputación de carácter corporativo. Así, en la Sentencia 139/1995, el Tribunal Constitucional establece que "la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando la difame o la haga desmerecer en la consideración ajena" (págs. 2-3).

Gracias a esta sentencia, es posible en España que las entidades u organizaciones puedan iniciar acciones civiles o penales tendientes a solicitar el retiro de contenidos de Internet cuando dichos contenidos suponen un menoscabo de su reputación.

No obstante, este derecho no es absoluto y puede entrar en conflicto con otros derechos, también recogidos en la Constitución Española, como el derecho a la libertad de expresión o el derecho a la libertad de información.

Algunos consejos prácticos

Crear una identidad digital corporativa no es fácil, requiere un trabajo constante y arduo cuyo objetivo es que los usuarios perciban una adecuada imagen de la entidad o la organización. De modo que la actividad de la entidad debe establecer unas pautas adecuadas relacionadas con:

- Una estrategia clara en torno a la identidad digital corporativa.
- Una política de interaccción con los usuarios: Requiere el establecimiento de una serie de medidas tendientes al establecimiento de una relación de confianza con sus usuarios así como un adecuado diálogo que permita el manejo adecuado de las críticas.
- Un estricto cumplimiento normativo: El incumplimiento de carácter normativo puede afectar la reputación debido a la imposición de sanciones derivadas de éste.
- La adopción de medidas de seguridad de carácter técnico y organizativo.

- Un adecuado protocolo de monitorización y seguimiento de la reputación online de la entidad u organización: Dicho seguimiento no sólo debe centrarse en aspectos tales como el posicionamiento en los buscadores o si la información que arrojan de dichos buscadores es positiva o negativa, también se debe monitorear y hacer un seguimiento activo en foros, blog, redes sociales, etc.

Lo dicho hasta ahora tiene que ver con recomendaciones de carácter preventivo pero… ¿Qué sucede cuando la entidad u organización se ve expuesta a una crisis de reputación digital? Es el momento de tomar decisiones y, en este sentido, pueden ser útiles las siguientes recomendaciones:

- Establecer un claro protocolo de actuación en caso de crisis: La entidad debe diseñar un protocolo o si se prefiere una orientación clara, detallada y correctamente implantada que permita a todos los funcionarios de la entidad saber exactamente qué hacer, cómo hacerlo y en qué momento, cuando se presenta una crisis.
- Usar los canales de denuncia apropiados, si es el caso: Los foros, las redes sociales y, en general, cualquier plataforma de carácter colaborativo tiene establecidos sus propios canales de denuncia que permitirán a la organización o entidad reaccionar frente a cualquier tipo de incidente o comentario que pueda menoscabar su imagen o reputación digital.
- Analizar la situación con el prisma jurídico, cuando los canales de denuncia citados sean insuficientes e iniciar las acciones que correspondan incluyendo, si es el caso, la denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado o ante los órganos judiciales correspondientes.

Identidad y reputación digital en la declaración de los derechos del ciberespacio

Una pequeña aproximación

Desde el mismo momento en el que una persona nace, adquiere una condición que prueba de la existencia de dicha persona como parte de la sociedad. Pero no se trata simplemente de una prueba de ello, también supone aquello que le caracteriza y lo diferencia, claramente, del resto de los seres humanos. Hablamos de la identidad.

Entre otros rasgos, que por ahora no interesan en el presente trabajo, podemos decir que la identidad de un ser humano se compone también de una serie de datos de carácter personal que le van a acompañar a lo largo de su vida. Estos son el nombre y apellido, la fecha de nacimiento, el sexo y la nacionalidad.

Cabe destacar que precisamente dicha identidad es la que permite a la persona, beneficiarse de la protección legal del país cuya nacionalidad ostente, en concreto.

En este sentido, vale la pena destacar de manera general, los pasos que se siguen para dotar de identidad completa a una persona, es decir, de una identidad a nivel jurídico:

- Obtención de la nacionalidad: puede ser originaria o de sangre, o por residencia; en todo caso, se obtiene mediante la inscripción de la persona en el Registro Civil correspondiente. Este acto administrativo le otorga un nexo de unión vital, no sólo con una determinada sociedad sino también con un Estado concreto y determinado.
- Obtención de la capacidad jurídica: Deviene de la inscripción en el Registro Civil así como de la concesión de la nacionalidad anteriormente citada. La adquisición de la capacidad jurídica permite a la persona ser reconocida como miembro de la sociedad y además le otorga, de forma inmediata, una serie de derechos y obligaciones.

Sin embargo, ¿qué sucede cuando una persona carece de nacionalidad y, por tanto, de capacidad jurídica? Aparece otro concepto jurídico: Apátrida. Un apátrida es una persona que carece de identidad oficial y que, por tanto, se torna en invisible a los ojos de la sociedad. Dichas personas debe enfrentarse a la exclusión y la discriminación así como a otro tipo de circunstancias desfavorables.

La identidad es de capital importancia para el ser humano ya que otorga la capacidad jurídica o, lo que es lo mismo, la personalidad jurídica. En definitiva, otorga la capacidad para ser sujeto de derecho.

Precisamente esa capacidad para ser sujeto de derecho es la que se encuentra protegida y reconocida como un derecho fundamental dentro de la Declaración Universal de los Derechos Humanos (ONU, 1948) que fue adoptada y proclamada el 10 de diciembre de 1948 y cuyo artículo seis establece que:

Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica.

En este sentido, podemos decir que la identidad, entendida como aquellos rasgos que caracterizan y diferencian a un ser humano y que le otorgan su capacidad jurídica, es un derecho fundamental de todo ser humano y, por lo tanto, debe ser reconocido en todas partes. De donde se desprende que la identidad también debe ser protegida en el ámbito digital, puesto que la identidad física puede tener su reflejo en el mundo digital, en Internet.

Protección de la identidad digital

La identidad, entendida como derecho humano fundamental se puede incardinar dentro de lo que se consideran derechos humanos de primera generación y que tratan, en esencia, de la libertad y la participación en la vida política. Son derechos de corte civil y político que pretenden proteger al ser humano de los excesos del estado.

Poco tiene que ver con los derechos de segunda generación, más encaminados o relacionados con la igualdad y cuya naturaleza tiene un claro corte social, económico y cultural.

Los derechos de tercera generación, tal y como postula el profesor Emilio Suñé Llinás[8] (2008) responden a las necesidades y valores específicos de las sociedades industriales avanzadas, cuya gran materia prima es la información y su quintaesencia, el conocimiento.

En este sentido, el profesor Suñé, también establece que todos aquellos derechos relacionados con el ciberespacio constituyen uno de los grandes núcleos de condensación de esta tercera generación de Derechos Humanos, directamente vinculada al cambio de valores que se produce en la nueva cultura postmaterialista, que en el ciberespacio es una cultura completamente desmaterializada.

---

[8] Emilio Suñé Llinás es Doctor cum laude en Derecho. Presidente del Centro Internacional de Informática y Derecho (CIID), entidad que promueve las rondas de la Convención Internacional de Derecho Informático. Participó en la Declaración de Lima, hacia la unificación de criterios normativos sobre protección de datos y privacidad en Iberoamérica.

Pues, precisamente esta desmaterialización, esta nueva cultura postmaterialista, es la que hace necesario que un derecho de primera generación, como el derecho a la identidad, también tenga su reflejo en los derechos de tercera generación, más aún cuando, hoy en día, ya no se puede concebir un ciberespacio en el que los seres humanos no tengamos derecho a nuestra identidad y a que nuestra información, entendida como aquel conjunto de datos, imágenes, registros, noticias, comentarios y un largo etcétera, tenga una adecuada protección jurídica ante injerencias de cualquier tipo.

Por esta razón considero que la identidad digital debe encontrarse regulada y tener su encaje en la declaración de derechos del ciberespacio que propugna el profesor Suñé, habilitando, para tal fin un nuevo artículo que contemple y regule la identidad digital.

Hemos de tener en cuenta que en ese metaespacio que es el ciberespacio, tal y como postula el Preámbulo de la Declaración de Derechos del Ciberespacio, que propugna el profesor Suñé (2008), no puede existir soberanía territorial alguna, y por tanto, dicha Declaración proclama la necesidad de establecer un orden de convivencia justo; de modo que la Declaración debería incluir no sólo nuevos considerandos sino también un nuevo artículo dedicado a la identidad y la reputación digitales.

Téngase en cuenta que la presente propuesta, compuesta de varios considerandos y un nuevo artículo, es un mero esbozo, una simple pincelada, que en todo caso debiera ser estudiada y analizada antes de su inclusión en la Declaración de los Derechos del Ciberespacio y que únicamente pretende ampliar el gran trabajo adelantado por el profesor Suñé.

Considerandos

Considerando que en la sociedad actual es tan importante establecer relaciones sociales en el mundo digital como lo es establecerlas en el mundo físico.

Considerando que la identidad digital es aquel conjunto de la información sobre una persona expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción en el plano digital de cada persona.

Considerando que de la identidad digital deriva el concepto de reputación digital.

Considerando que identidad y reputación digital deben ser no sólo reconocidas sino también protegidas ante los posibles riesgos o amenazas a los que puedan verse expuestas.

Protección de la Identidad Digital

1. Toda persona física tiene derecho al reconocimiento de su identidad digital así como al reconocimiento de su reputación digital.
2. Para su correcta protección, se deberán habilitar las garantías institucionales, tal y como establece el artículo 20 de la presente declaración, que sean necesarias para evitar riesgos o amenazas a la identidad digital tales como la suplantación de identidad, la violación de la intimidad o cualesquiera otros riesgos presentes o futuros que puedan amenazarlas.
3. Corresponde a la persona física velar y cuidar de su respectiva identidad y reputación digital, como mecanismo para evitar los riesgos o amenazas a los que puedan verse expuestas.

Trabajos citados

Alonso, J. (2011). Identidad y reputación digital. En P. Cerezo (Ed.), Cuadernos de comunicación Evoca, 5. Identidad digital y reputación online (págs. 5-10). Madrid, España.

Gamero, R. (2009). La configuración de la Identidad Digital. notaenter-ie. No.131, junio, 1-6.

Giones-Valls, A., & Serrat-Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital. BiD: textos universitaris de bibliotecnomoia i documentació. No.24, junio, 1-15.

INTECO. (2012a). Guía para usuarios: Identidad digital y reputación online. España: Instituto Nacional de Tecnologías de la Comunicación, Gobierno de España, Ministerio de Industria, Energía y Turismo.

INTECO. (2012b). Guía para empresas: Identidad digital y reputación online. España: Instituto Nacional de Tecnologías de la Comunicación, Gobierno de España, Ministerio de Industria, Energía y Turismo.

Ley 34/2002. (2002). De servicios de la sociedad de la información y de comercio electrónico. Madrid: BOE No. 166 de 12 de julio.

ONU. (10 de diciembre de 1948). Declaración Universal de Derechos Humanos. Obtenido de ONU Naciones Unidas: http://www.un.org/es/documents/udhr/

Rundle, M., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., y otros. (29 de febrero de 2008). At a Crossroads: "Personhood" and Digital Identity in the Information Society. Obtenido de OECD: www.oecd.org/dataoecd/31/6/40204773.doc

Sentencia 139. (1995). Sentencia 139/1995, Jurisprudencia Constitucional. Madrid, España: Publicación BOE: 19951014 [«BOE» núm. 246].

Sentencia 292/2000. (2000). Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Madrid: Boletín Oficial del Estado.

Suñé, E. (2008). Declaración de derechos del Ciberespacio. Madrid: Universidad Complutense de Madrid.

Velich, A., Huel, P., Bastidas, P., & Fernández, M. (27 de junio de 2010). Siete principios constitutivos de las aplicaciones web 2.0. Obtenido de WEB 2.0: http://web20tp.blogspot.com.co/2010/06/siete-principios-constitutivos-de-las.html