Manejo de Identidad en Internet

Laura Raquel Vaesken Zaracho

Universidad Católica "Nuestra Señora de la Asunción"
Facultad de Ciencias y Tecnología
Teoría y Aplicación de la Informática 2
Asunción - Paraguay
Octubre 2016

Resumen La identidad es lo que nos define como individuos y nos permite diferenciarnos de los demás. Así mismo, desde el momento en que dejamos rastros en la web también ya poseemos una identidad digital. Este documento trata sobre la identidad en Internet: descripción, características, manejo y posibles peligros e implicancias que se pueden presentar.

Key words: identidad, identidad digital, Internet, huella digital, privacidad, reputación, visibilidad, seguridad.

1. Introducción

La identidad en Internet es toda aquella información publicada sobre un individuo en Internet y que se genera y comparte usando medios digitales y tecnológicos. Es una información dinámica que evoluciona en función de las interacciones del usuario y de la información que se publique sobre uno mismo. Generalmente, no desaparece por el paso del tiempo y es accesible para cualquiera. [1]

El conocimiento sobre la identidad en Internet y su manejo se ha vuelto cada vez más importante con el aumento de nuestra presencia en Internet y también el aumento de la actividad criminal online. En el nivel más simple, la identidad digital es un suplemento a la identidad real del individuo. En otras palabras, se puede decir que la identidad digital es un conjunto de credenciales o atributos que permiten a un tercero evaluar y verificar la autenticidad de la identidad en cuestión y las demandas planteadas por ella. Por ejemplo, si se permite o no el acceso a un determinado sitio web o se permite realizar un pago.

Por otra parte, las identidades digitales pueden variar desde un solo atributo o credencial, como la edad, a algo complejo, como ser los detalles de la cuenta bancaria del hogar. Sin embargo, la principal diferencia entre identidades físicas y las identidades digitales tiende a ser el volumen de datos. Donde la mayoría de la personas tiene 3-4 documentos de identificación -credencial de identificación, pasaportes- el numero de identificaciones digitales tienden a ser un número

grande y creciente - cuentas múltiples de correo electrónico, Facebook, Google y accesos a otros medios sociales. [2]

2. Marco Teórico

Desde las últimas décadas del siglo pasado, se ha producido una revolución tecnológica a escala mundial que ha dado paso a una sociedad informacional, definida por la generación, la gestión y el uso de datos. La revolución actual gira en torno a las tecnologías del procesamiento de la información y la comunicación, que, cada vez más, se usan en la mayoría de ámbitos de nuestra vida. Con la eclosión de Internet y sobre todo de la denominada web 2.0, la cantidad de datos personales existentes en la red es muy elevada y contribuye a crear nuevas identidades personales en el entorno digital que, como veremos, pueden coincidir o no con la identidad analógica, es decir, con las características que se pueden atribuir a una determinada persona en su vida fuera de la red o offline. La irrupción de Internet ha ofrecido una gama amplísima de nuevas herramientas para la creación de contenidos y de comunicación cambiando las condiciones tradicionales de gestión de la identidad.

Actualmente, la capacidad de enviar y gestionar datos aumenta y el consumo informativo no sólo es ingente en empresas y en el ámbito comercial, sino que la cantidad de datos que un individuo genera, gestiona, edita o comparte cada día es difícilmente calculable . Ante la gran abundancia de información y de la sobreexposición a los demás, el individuo queda desprotegido. Es por ello que recientemente se ha reactivado el debate sobre la necesidad de formar a las personas en nuevas alfabetizaciones, informacionales y digitales, que se convierten en clave para los ciudadanos de hoy.

Los llamados nativos digitales son el paradigma de generación que utiliza de manera intensiva Internet. Es la generación nacida a partir de la década de los años noventa y que no ha conocido la vida sin la red, también se ha denominado generación Google, entre otros nombres. Usan Internet diariamente para una variedad creciente de propósitos y tienden a preferir el ordenador antes de que la libreta y el lápiz. Cabe decir, sin embargo, que estos jóvenes digitales se caracterizan también por ser exhibicionistas y multitareas, y, por ejemplo, lo que hace una década era un diario personal o una conversación privada, ahora se ha convertido en un blog o unos mensajes publicados en una red social. La comunicación mediante el ordenador (CMC) se convierte en la sustitución y la complementariedad de otros canales tradicionales teniendo en cuenta que la electrónica permite que la información sea visible y replicable para mucha gente. Con todo, lo más destacable de la generación Google es que son productores y consumidores de información en Internet: para el ocio, para los estudios, para las relaciones personales y a menudo para todo a la vez.

Estar en el ciberespacio significa tener una representación de uno mismo, una identidad digital que se va construyendo a partir de la propia actividad en Internet y de la actividad de los demás. La oferta actual de ocio/negocio y consumo cultural en Internet, las aplicaciones para la comunicación electrónica y los sitios de redes sociales construyen una estructura en la que vive un “yo virtual".

Nuestra huella digital está formada por los rastros que dejamos al utilizar Internet. Todos los días la mayor parte de las personas contribuye a crear un retrato creciente de quiénes son en línea. Este retrato ayuda a las empresas a orientar los contenidos hacia mercados y consumidores específicos, ayuda a los empleadores a analizar antecedentes y ayuda a los anunciantes a seguir nuestros movimientos a través de múltiples sitios web. Sin importar lo que hagamos en línea, es posible que estemos dejando atrás nuestras huellas digitales.

Ese rastro que conforma nuestra identidad digital está formado por una serie de impactos de distinta procedencia. La identidad digital se puede configurar de muchas maneras y una misma persona puede tener diferentes identidades utilizando herramientas diversas o tener sólo una. Algunos de ellos son los siguientes:

- Sitios web y compras en línea: A menudo las tiendas minoristas y sitios de reseña de productos dejan en nuestro sistema cookies que pueden seguir nuestro recorrido de un sitio a otro, permitiendo la entrega de anuncios dirigidos que nos muestran productos sobre los cuales hemos estado leyendo o que hemos buscado recientemente.
- Redes sociales: Todos esos +1, retweets y comentarios en Facebook (incluso los privados) dejan un registro. Es importante conocer cuáles son las configuraciones de privacidad por defecto de nuestras cuentas en las redes sociales y estar atentos a las mismas. Muchas veces los sitios introducen nuevas políticas y configuraciones que aumentan la visibilidad de nuestros datos. Puede que confíen en que el usuario simplemente hará clic y aceptará todos los términos que están introduciendo, sin siquiera leerlos.
- Teléfonos móviles, tablets o computadoras portátiles: Algunos sitios web generan un listado de los diferentes dispositivos que utilizamos para acceder a los mismos. Aunque muchas veces esto se utiliza como una forma de ayudarnos a proteger nuestras cuentas, es importante comprender qué información recogen sobre nuestros hábitos. [3]

La identidad digital puede mostrar cómo es de diversa la propia vida y como es de múltiple la propia identidad. Una misma persona puede tener diferentes identidades, por ejemplo, como fan de un grupo de música internacional, como miembro de una comunidad religiosa y como integrante de una saga familiar. Estas tres identidades pertenecen a una misma persona y eso se puede ver fácilmente reflejado en Internet.

Actualmente, se pueden encontrar con facilidad los datos y los productos de la actividad de una persona en la red de manera fragmentaria, es decir, fotos en un fotolog, opiniones personales en un foro o direcciones de correo electrónico y

teléfonos en una red social. Así mismo, también hay webs gratuitos que recogen toda la información de una misma persona y la muestran ordenadamente según el tipo de datos. Sitios como pipl.com o 123people.com suelen ofrecer todo tipo de datos, incluso a través nubes de palabras con los conceptos que más identifican a una persona.

3. Visibilidad y Reputación

Toda actividad que genera un individuo en la red constituye su visibilidad, que puede ser positiva o negativa. Esta visibilidad puede ser autoconstruida a partir de los posts de un blog, los mensajes de Twitter, los comentarios a vídeos, fotos ..., pero también puede ser fruto de referencias o comentarios de terceros. La comparación en el mundo analógico sería si la persona es más o menos conocida.

Nos interesa ser visibles? Queremos pasar inadvertidos o aprovechar la ubicuidad que permite la red para estar en todas partes? Es determinante decidir qué tipo de presencia, qué tipo de visibilidad digital nos interesa.

Un ejemplo para aumentar la visibilidad personal es utilizar el servicio de Google Latitude, basado en Google Maps, es una herramienta que aumenta la visibilidad de los usuarios más allá de su círculo social, ya que el individuo que activa este producto se convierte localizable físicamente en un mapa y puede contactar con otros individuos que también hayan geolocalitzado con este servicio a través de la web o desde un dispositivo móvil.

Otro ejemplo de visibilidad muy utilizado por bloggers o personas que actualizan informaciones regularmente es enviar la noticia de actualización de estos contenidos por correo electrónico a través de sitios de redes sociales u otras herramientas. Esta es, sin duda, una manera muy eficaz de compartir los materiales en la red y de maximizar la posible audiencia.

El impacto que tiene la visibilidad de una persona en el mundo digital es medible, por ejemplo, a partir del número de contactos que tiene, o bien, por los seguidores que tienen ciertas actividades. También es medible a partir de las veces que unos determinados contenidos son replicados, por ejemplo, al replicar la entrada de un blog, comentar un vídeo, los contenidos colgados en una red social, etc. Por otro lado, se trate o no de un web colaborativo, el tráfico que genera constituye un indicador de visibilidad cuantificable, así como el número de enlaces que lo apuntan.

Es por ello que cabe preguntarse hasta qué punto es visible la propia “marca personal", nuestro nombre. Para las empresas, el solo hecho de generar señales de cualquier tipo ya se tiene en cuenta como una acción de marketing; a escala

personal, hay que valorar si esto es algo beneficioso o no.

El antropólogo Robin Dunbar explicó que el límite cognitivo de relaciones sociales estables que un ser humano puede mantener es aproximadamente de 150. Este número, conocido como el número de Dunbar, actualmente también se aplica al número de contactos virtuales, en sitios de redes sociales, foros o comunidades virtuales. Aced afirman que “un usuario de Internet obtiene visibilidad absorbiendo información, procesando y compartiéndola con el resto de usuarios, siempre que sea útil y valiosa para los demás".

La reputación recae en la opinión que otras personas tienen de un sujeto. Sin embargo, la construcción de esta reputación también puede hacerla, en parte, el propio interesado. ¿Quién no mira antes de elegir un hotel, reservar una mesa en un restaurante o comprar un libro qué es lo que otros han dicho? Para encontrar respuestas y elegir la que más nos interesa recurrimos a la reputación, así las opiniones de terceros pueden influir en nuestra decisión de compra.

Trasladado al mundo analógico sería ver si una persona (o empresa) goza de buena o mala prensa. Según Solove, la reputación es “un componente clave de nuestra identidad, refleja quiénes somos y define cómo interactuamos con los demás".

En este sentido, toma importancia el hecho de tener presente quién habla de quién, en qué sitios y de qué manera. No es lo mismo la opinión de una persona poco visible, que la opinión de una persona muy visible, que difundirá sus juicios de manera más rápida y probablemente a su vez a personas también más visibles. Según Aced, “la autoridad y el estatus no se consiguen por jerarquía, sino por la capacidad de estar conectado de forma interactiva con otras personas, es decir, recibiendo y emitiendo mensajes interesantes para los demás".

LinkedIn es una red social con una clara orientación profesional y una buena herramienta para gestionar la reputación en Internet. En esta red cada usuario crea un perfil y se puede comunicar con personas de su campo o círculo profesional. Entre las múltiples funcionalidades que ofrece, existe la posibilidad de recomendar una persona y añadir un comentario con una breve explicación sobre cuáles son sus cualidades profesionales. En este entorno, un profesional en paro pero con buenas recomendaciones en LinkedIn tendría más posibilidades de encontrar trabajo.

Algunas de las herramientas de reputación electrónica, según Bancal, son los motores de búsqueda de blogs, los meta motores sociales, las herramientas de seguimiento de comentarios, las herramientas de microblogs, los agregadores sociales o redes sociales y los motores de búsqueda de personas.

4. Privacidad versus Autenticidad

Facebook y Google quieren enlazar las personas online y offline mientras que 4Chan y otros sitios sociales prefieren que las personas jueguen con la libertad de pseudónimos.

Antes de que Facebook y Google se convirtieran en los gigantes de la web, el más famoso adagio en la web era: “En el Internet, nadie sabe que eres un perro". Los días en que las personas se les permitía ser perros está llegando a su fin aparentemente. La antigua web, un lugar donde la identidad podía permanecer separada de la vida real, está desapareciendo rápidamente de la pantalla del ordenador. De acuerdo con Sheryl Sandberg, directora de operaciones de Facebook, y Richard Allan, director de la política en Europa, una masa crítica de personas sólo quieren interacciones en línea con el apoyo de la identidad “auténtica". Y esto, dicen los críticos, tendrá efectos irrevocables a la apertura de la web.

La búsqueda de la autenticidad se está arrastrando en el corazón de la mayoría de los modelos de redes sociales y en el panorama actual de Internet está jugando un papel importante en cómo nos relacionamos unos con otros y con el contenido web. Para muchas personas, los productos de Facebook y Google son la suma total de su interacción web, y el valor en la creación de una plataforma que proporciona la confianza de que una persona es quien dice ser, ante alguien que pretende ser ellos, es fundamental para el éxito de una red social.

Dentro de este modelo, la identidad autentica es no-anónima. Perfiles de Facebook e identificaciones con Google están ligados a nombres reales de personas y conexiones reales, y cada vez más a sus actividades en todo el ciberespacio. Los usuarios están familiarizados con la sesión en otros servicios que utilizan Facebook o ID de Google, formando una única identidad pública que es una versión agregada de su pasado fuera de línea, la online actual y sus futuros combinados.

Facebook también cree autenticidad está vinculado a la conjunto de fotografías de una persona, por lo que recientemente acaba de pagar 1.000 millones de dólares para el servicio de compartición de fotos Instagram. “Las imágenes dicen más que mil palabras", dice Allan. “Los funcionarios de inmigración le pueden pedir ver un álbum de fotos para ver si una relación es genuina. Es una forma muy instintiva y de gran alcance para confirmar la identidad auténtica."

No todo el mundo está de acuerdo. “Yo no diría que lo que tienes en Facebook “identidad auténtica", dice Christopher Poole, creador de 4Chan, una comunidad en línea fundada en 2004. 4Chan cuenta con dos características de diseño antitéticas a Facebook: en primer lugar, su 20 millones de usuarios no registran una cuenta para participar y por lo tanto son anónimas; En segundo lugar, no hay ningún archivo.

Poole, que fue elegido como la persona más influyente de la revista Time de 2008 - dos años antes de Facebook, Mark Zuckerberg, fue declarada por la revista Hombre del Año - cree que las motivaciones comerciales de Facebook cerraron la experiencia en línea: “Mark y Sheryl han salido y dijeron que la identidad es autenticidad, quien sos online es lo mismo de quien sos cuando estas offline, y tener múltiples identidades tiene faltante de integridad. Creo que es una locura". “Pasamos de una red que fue impulsado por el interés, y luego la transición a una web en la que las conexiones eran en persona, relaciones de amistad en la vida real", añade Poole. “Los individuos son multifacético. La identidad es prismática, y existen comunidades como 4Chan como un vestigio de la web orientada por los intereses."

Sin embargo, el éxito de una red social no tiene por qué depender de esta relación directa entre la identidad en línea y fuera de línea. En Japón, las tres redes sociales más populares operan bajo pseudónimos a discreción del titular de la cuenta. “[Redes sociales japonesas] son anonimas, pero podemos rastrear pasadas por ID de inicio de sesión o apodo,.explica Yasutaka Yuno, editor en jefe del sitio más popular tecnología móvil de Japón, K-tai Watch. “El menciones pasadas son útiles para juzgar la credibilidad. En cada comunidad social, ID actúan como nombre real de personas."

Una identidad en línea puede ser tan permanente como una fuera de línea: los usuarios con pseudónimo a menudo se identifican en las diferentes redes sociales utilizando el mismo nombre de cuenta. Pero debido a que sus alias no están basados en nombres reales, pueden delinear deliberadamente su identidad en consecuencia, y reafirmar el anonimato si así lo desean. Este tipo de actividad se permite incluso en países donde los titulares de las cuentas de redes sociales son obligados a usar un documento nacional de identidad para registrarse en un servicio, como en Corea del Sur y China; sus identidades públicas en línea siguen siendo fabricaciones. Incluso con este vínculo explícito con el estado, cuando los usuarios son conscientes de que sus actividades en línea son trazables, el juego de la identidad continúa.

Andrew Lewman, director ejecutivo del Proyecto Tor, espera volver a anonimizar la web. “La capacidad de ser anónimo es cada vez más importante, ya que proporciona un control a las personas, les permite ser creativos, les permite averiguar su identidad y explorar lo que quieren hacer, o para investigar temas que no son necesariamente ’para ellos’ y tal vez no quiera tener ligado a su nombre real a perpetuidad", dice.

El navegador y el software de Tor impide que el tráfico web de un usuario pueda ser rastreado, saber quién es usuario o de dónde vienen, a través del rebote de las comunicaciones de un individuo a través de al menos tres lugares diferentes. La gente todavía puede ser identificada en un servicio como Facebook o Google, si así lo desean conectarse, pero Tor evita que estos sitios puedan saber

que los usuarios estaban haciendo antes, y hacia dónde van después de cerrar la sesión.

Esta es una solución tecnológica para lo que Lewman siente es un problema elemental con la des-anonimización de la web. “La capacidad de olvidar, para empezar de nuevo es importante", argumenta. “Tal vez lo que se divorciaron, tal vez usted acaba de salir de rehabilitación y quiere empezar de nuevo.

“Si realmente quiere ser anónimo, tendría que utilizar una combinación de 4Chan y Tor", explica Poole. Tor proporciona el anonimato back-end que complementa el anonimato front-end de 4chan. Pero esto es tecnológicamente avanzado. Y así, la batalla ideológica sobre la identidad en línea continua.

“Facebook está fijando las expectativas de lo que queremos", dice Poole. “Ellos definen el nivel y tipo de control que sus usuarios tienen sobre su identidad en línea. Ellos han estado limitando y disminuyendo ese nivel de control de forma lenta pero segura en una dirección que se podría llamar la transparencia, pero otras personas pueden llamar falta de opciones."

Allan cree que los beneficios de la identidad auténtica son mayores a los costos. Facebook y otros servicios ofrecen garantías de seguridad y credibilidad que son más inclusivas, y abren la web a un nuevo público que nunca habría ido en línea antes, dice. “Somos optimistas. Facebook permite a cientos de millones de personas a expresarse en línea porque no tienen o no saben cómo utilizar las herramientas que necesitaban."Facebook, en su opinión, es un trampolín para el resto de la web. [4]

5. Derecho al olvido

El derecho al olvido se podría definir como el derecho que tiene el titular de un dato personal a borrar, bloquear o suprimir esa información personal, que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales, como el derecho a la intimidad, al honor y a la propia imagen, o que podría considerarse como información obsoleta, pues carece de sentido que se tenga acceso a ella después de mucho tiempo y ya no sirve a los fines para los que fue recabada y publicada.

Mario Costeja González pasó cinco años luchando para tener 18 palabras eliminadas de la lista de resultados de búsqueda de Google en su nombre. Cuando el español se había buscado en Google a sí mismo en 2009, dos resultados importantes aparecieron: avisos de ejecución hipotecaria en casa de 1998, cuando estaba en problemas financieros temporales. Los avisos se habían publicado en el diario español La Vanguardia y recientemente digitalizado. Pero su propósito original - atraer a los compradores a subasta - había caducado hace una década, al igual que la deuda. Costeja González pidió el periódico para eliminarlos.

Cuando eso no tuvo éxito, desafió a Google, y el caso fue finalmente elevado a la Corte Europea de Justicia, máximo tribunal de Europa. La crudeza de la naturaleza atemporal de memoria digital - y el poder incuestionable de empresas privadas, por motivos comerciales que lo controlan - era un reto que el hombre de 59 años de edad, Costeja González decidió abordar directamente.

En mayo de 2014, el Tribunal de Justicia falló en contra de Google. Se reconoció que cuando ingresamos el nombre de alguien como una consulta de búsqueda, momentos dispersos de su vida se presentan de manera mecánica, con un significado distorsionado por falta de contexto, haciendo una construcción de un perfil detallado, pero selectiva. ¿Cuáles son los derechos de las personas a las que se refieren los perfiles? ¿Y cuáles son los derechos de los solicitantes de información?

La cuestión produce una división filosófica interesante. Una posición es que una vez en línea, la información debe permanecer en línea (excepto cuando es ilegal en virtud de la difamación, derechos de autor, o el derecho penal). Este es generalmente el punto de partida de la mayoría de las compañías de Internet de Estados Unidos, organizaciones de libertad de expresión y los medios de comunicación; una vista típica de aquellos criados en los Estados Unidos bajo Primera Enmienda.

Por otro lado, hay toda clase de razones para eliminar los datos, distintos de ser obligado por la ley. Uno podría querer eliminar la información por razones emocionales, razones éticas, o "porque sí", cuando no hay un interés compensatorio. Algunas solicitudes recientes de eliminación aprobados por Google incluyen las historias clínicas de los pacientes; íntimas fotos privadas; antiguas conversaciones de grupos privados que terminaron en línea.

En el mundo real, los sedimentos de información a través del tiempo, dan a la gente la capacidad de seguir adelante, para recordar, pero no están agobiados por su pasado. Fuera de línea, nos comunicamos de diferentes maneras con diferentes "públicosz propósitos.

Y ésta era la opinión del Tribunal de Luxemburgo, que ofrece en su justificación de la ley de protección de datos de la UE. El tribunal dictaminó que los datos personales deben ser retirados de los resultados de búsqueda en el nombre de una persona cuando anticuado, inexacto, inadecuado, irrelevante o sin objeto, y cuando no existe un interés público.

Un interés público demanda que la información relevante sigua siendo accesible, por lo que la información pertinente acerca de los políticos electos, funcionarios públicos, profesionales y criminales – e incluso sólo malas críticas - todo con justificacion se encuentren accesibles, por lo tanto, Google rechaza dichas solicitudes.

La frase “derecho al olvido"se menciona sólo brevemente en la sentencia, pero fue inmediatamente analizada por los medios, Google y los reguladores. A pesar de que ha sido sustituido por el “derecho a suprimir de la lista de resultados"más precisamente, el impacto de la etiqueta de “derecho al olvido.erra forzar el debate en los binarios: olvido vs recuerdo, privacidad vs libertad de expresión, la censura vs la verdad o historia. Estos son falsas dicotomías, insuficientemente matizada de hacer frente a la realidad de nuestras vidas y las complejidades de la existencia humana.

El punto es tener derechos frente a los motores de búsqueda no es manipular la memoria o eliminar la información, pero para que sea menos prominente, cuando esté justificado, y combatir los efectos secundarios de este fenómeno exclusivamente moderno que la información es instantánea, a nivel mundial, y accesible a perpetuidad.

¿Desde cuando el Internet se ha convertido en “verdad", o “memoria¿ ¿Y desde cuándo tiene “historiareducido a la lista priorizada en los resultados de Google de una colección imperfecta de las huellas digitales? Tales elisiones ignoran el matiz del perdón y la comprensión, en conjunción con la memoria misma, en la construcción de la verdad y la justicia. Subestiman la privacidad y la autonomía, al precio de casi total transparencia, en la construcción de la comunidad y la seguridad.

Los encuadres de todo o nada impuestas en este caso limitan, la influencia y dan forma a la narración de una guerra mucho más amplia: la lucha por nuestras identidades digitales. Hemos llegado a un momento crítico. El control sobre nuestros datos personales esta casi perdido en línea: perdido frente las corporaciones, los gobiernos; perdido entre sí. ¿Cómo podemos, como individuos, estar habilitadas por los enormes beneficios de la conectividad digital y los flujos de información global, per aun conservar cierto control personal sobre la forma en que nuestras identidades están representados y se negocian en línea? El caso de Costeja González es un pequeño pero crítico batalla en ese terreno más amplio.

Nueve meses después de la decisión europea, es evidente que la implementación de Google ha sido rápido, idiosincrásico, y es permitido a la compañía dar forma a la interpretación de sus propios fines, así como para obtener una ventaja sobre los competidores y reguladores forzados al modo reactivo.

Un poco más de dos semanas después de la sentencia, Google lanzó un formulario en línea para que los ciudadanos identifican vínculos de los resultados de búsqueda de sí mismos que seab “irrelevante, obsoleta o de otra manera cuestionable solamente una lectura parcial de la ley que rige, que también incluye “incorrecta, inadecuada o engañosa". Comenzó a eliminar los enlaces un mes más tarde. En el momento de escribir esto, la empresa había recibido 218,427 solicitudes, que comprende un total de 789,496 enlaces. Se ha llegado a una decisión

sobre el 83 % de los enlaces y de hecho fueron eliminados 264.450 de ellos, o el 34 %. Sin embargo, todo esto se ha hecho sin revelar sus procesos internos, los criterios de eliminación o cómo se está dando prioridad a los casos. [5]

6. Gestión eficaz de la identidad en Internet

Hay dos perspectivas para aproximarse al tema de la identidad digital y de Internet. Una es creer que la presencia virtual significa un peligro para la seguridad personal y, por tanto, convenir en que si un individuo no construye su identidad digital, una tercera persona puede suplantarla y pueden ocurrir hechos indeseables. La otra perspectiva es entender la construcción de la identidad en la red como una oportunidad de aprendizaje tanto personal como profesional dentro de la cultura informacional donde vivimos inmersos.

En general, las personas quieren ser homogéneas, es decir, mostrarse de la misma manera en las diferentes facetas de la vida, ya sea analógica o digital, teniendo en cuenta que cada vez todo aquello que corresponde a la esfera personal y a la esfera virtual tiende a imbricarse más. Es por ello que podemos hablar de una identidad híbrida (analógica y digital) y que el conjunto de ambas es, efectivamente, la propia identidad, una única identidad. Actualmente, la gran diversidad de servicios web y herramientas en Internet hace que generalmente las identidades digitales estén fragmentadas. Este hecho, sin embargo, no significa en ningún caso que una persona no tenga una sola identidad en Internet.

Para gestionar eficazmente la identidad digital hay que tener presente que:

- Una identidad digital personal es una representación virtual que nos permite interactuar en el ciberespacio, proyectar una personalidad y difundir una trayectoria personal o profesional para aprender y compartir información, como noticias, webs, aficiones, opiniones, etc.
- Es posible no querer tener una identidad digital y no participar activamente en la nueva cultura digital. Esta es una opción personal, no obstante, que no garantiza que otras personas hablen o publiquen material de un individuo determinado, o bien suplante su identidad en Internet.
- Si bien es cierto que la propia identidad digital debería ser totalmente coherente con la identidad analógica, también es verdad que el entorno virtual puede ser el escenario idóneo para realizar algunas actividades concretas, como desarrollar una afición o encontrar contactos estratégicos para a una determinada actividad profesional. También cabe destacar que la generación digital ya no diferencia entre la identidad digital y la analógica y, según apunta Freire, tampoco haremos esta distinción en el futuro.
- Todo lo que se publica en Internet queda para la posteridad, hecho que puede tener consecuencias futuras en la imagen y la reputación personal. Lo que se difunde sobre uno mismo y lo que nos rodea contribuye a escribir una memoria colectiva y perenne en la red. Son numerosas las quejas de los ciudadanos del peligro que puede llevar que un documento quede en la red

a lo largo de los años. Este fue el caso de un profesor de Farmacología de Buenos Aires, que después de escribir su nombre en un buscador, el primer resultado era de la base de datos Dialnet con sus once libros escritos, pero el segundo era una noticia publicada por un rotativo en 1988 sobre el ingreso en prisión por un asunto relacionado con la organización ETA4. En el archivo del periódico, aparecían catorce noticias con su nombre, pero ninguno informaba del desenlace del proceso. El hecho es que el rastro de la identidad digital en la red no se borra fácilmente, y es justamente por este motivo que diarios como El País reciben a menudo cartas de lectores que, conscientes de lo que supone que salga su nombre en una noticia, piden que se les borre de los índices de búsqueda.

- Crear una identidad digital significa entender la tecnología y participar de ella. Es una oportunidad para demostrar quiénes somos realmente y acercarnos a la gente con intereses o aficiones similares.
- Al igual que ocurre en el mundo analógico, hay buenas razones para tener varias identidades digitales en contextos diferentes. Pero experimentar otras identidades, a través de seudónimos y avatares, es también un riesgo, del mismo modo que alguien puede engañar, también puede ser engañado.
- La credibilidad y la confianza, en el mundo virtual, también se gestionan aportando información responsable y ética. Apareció en las noticias que en Marruecos un joven ingeniero civil de 26 años, Fouad Mourtada, se hizo pasar en diferentes sitios de redes sociales por el príncipe Moulay Rachid, hermano menor de Mohamed vi. Este hecho acabó con la condena del ingeniero a tres años de cárcel y a pagar 900 euros de multa en el tribunal de primera instancia de Casablanca.

La gestión de la identidad digital implica que los usuarios sean conocedores del entorno web y que participen éticamente. Cuando somos conscientes de estas premisas y de las oportunidades y peligros de la red a la hora de gestionar la propia información personal se puede garantizar la gestión adecuada de la identidad personal y una mejor "calidad de vida.[en] la sociedad del conocimiento. Hay que tener presente que este conocimiento no sólo implica la participación del usuario sino también la de las entidades y empresas que hay detrás de estos servicios, que día a día son más conscientes de los problemas de seguridad y privacidad de los datos en la red.

Hoy en día Internet ofrece numerosas soluciones telemáticas, como facturación electrónica, visado digital, voto electrónico, firma electrónica, carné de identidad digital, formularios telemáticos, certificado digital, receta electrónica, etc., todas ellas opciones basadas en la encriptación de datos y en la utilización de dispositivos inteligentes como claves, tarjetas y generadores de contraseñas, que permiten la autenticación. El protocolo implantado es el HTTPS (hypertext transfer protocol secure), un sistema cifrado para transferir archivos confidenciales que incluyen datos personales o financieros. La política actual de protección de datos supone que los usuarios deben aceptar explícitamente las condiciones de los servicios digitales a los que acceden, y que se responsabilizan de la veracidad

de los datos que aportan, mientras que las empresas e instituciones que disponen de sistemas de recogida y gestión de datos personales deben garantizar que el sitio cumple con los requisitos de protección y privacidad de los datos que reciben.

A pesar de las medidas preventivas, la usurpación de la identidad y el uso fraudulento son problemas comunes en el mundo virtual. Delitos frecuentes son los relacionados con falsas identidades, como el robo de identidad, los fraudes y los plagios. Un hacker tiene la capacidad de revelar y mejorar el funcionamiento de un sistema de seguridad, e incluso puede contribuir a detectar webs que desarrollan actividades delictivas, como plataformas con contenidos pronazis o pederastas. El cracker (o pirata informático), en cambio, utiliza los conocimientos para vulnerar los sistemas de seguridad ajenos y obtener cierta información que le reporta un beneficio. Es así como puede llegar a hacer usos fraudulentos como el phishing, una modalidad de estafa por correo electrónico diseñada para acceder de manera fraudulenta a cuentas bancarias. Los mensajes contienen formularios, o remiten a un sitio web de apariencia similar al de la entidad pero que no es real, sino una copia. Se pide al destinatario que vuelva a introducir datos confidenciales y claves financieras, y de esta manera se puede acceder sin problema a la cuenta bancaria. Hay que tener presente que una entidad bancaria nunca pide esta información por correo electrónico. El phishing y las técnicas para conseguir claves de sistemas informáticos o tarjetas de crédito se incluyen dentro de las prácticas de ingeniería social, las cuales tienen como objetivo obtener información confidencial haciendo uso del engaño y la manipulación de los usuarios legítimos. Ante los ataques, a través de Internet o del teléfono, de los cracker sólo es posible defenderse con un aprendizaje sobre el uso ético y legal de los datos personales y de la seguridad en Internet.

En este apartado se muestran diferentes herramientas y sitios de la Web 2.0 estrechamente ligados con la identidad digital.

- Herramientas para homogeneizar la propia presencia en la red
  — OpenID
  OpenID es una manera de autenticarse en las páginas web sin la necesidad de tener un usuario para cada una de las plataformas. Es así como permite que el usuario gestione su identidad digital de manera centralizada, evitando la esquizofrenia digital de utilizar diferentes identidades y que se tengan que memorizar grandes cantidades de información para identificarse en los diferentes servicios en línea. OpenID es abierto y defiende la autenticación única de los usuarios en la red. Hay empresas que al detectar también estas deficiencias han creado los propios servicios de autenticación pero simplificando y mejorando la experiencia del OpenID.
  Hay que tener cuidado, no obstante, porque el hecho de tener unificada la identidad digital hace que sea más vulnerable en caso de que alguien averigüe la contraseña de acceso.

— Facebook Connect
Facebook Connect es un gestor de identidades aplicable a diferentes páginas web a partir del cual cuando un usuario deja un comentario puede hacer que automáticamente quede reflejado también en su perfil de Facebook. De este modo puede compartir la información que encuentre de interés con los contactos de Facebook.

— Google Friend Connect
Google Friend Connect es un módulo ofrecido por Google para añadir una capa social en cualquier blog (parecido a Facebook Connect), al mismo tiempo también añade una autenticación desde otra cuenta como la de Twitter, de modo que los visitantes del blog podrán utilizarlo para twittear sin tener que salir del bloque.

- Identificar perfiles de personas concretas
Estas herramientas sirven para autentificar que la persona es realmente quien dice que es.

— Identify: agregador de Firefox para investigar personas
Identify es un complemento del navegador Firefox que busca todos los perfiles de un usuario a todos los sitios de redes sociales y los aglutina en una única interfaz (es preciso que el usuario haya elegido previamente un mismo nombre para identificarse). Una vez instalada la aplicación en el navegador Firefox, si se busca Oprah Winfrey, nombre de la popular presentadora americana, aparece como primer resultado su Twitter y se puede ver como Identify lo marca como “perfil verificado". Ciertamente, es su verdadero perfil por el número de seguidores que tiene, pero se encuentran más resultados si se busca por el mismo nombre, la mayoría de los cuales son identidades falsificadas de la popular presentadora.

- Integrar mensajes de una plataforma a otra

— Twit This
Twit This ofrece una manera fácil de publicar una noticia de un blog en el canal de Twitter. Para harcerlo, es necesario que el blog o la web incluya la opción Twit This y sólo hay que hacer clic e identificarse en Twitter. Una vez hecho esto, el mensaje de un blog se puede publicar en el propio canal de Twitter y así hacerlo visible a todos los contactos de este canal. Además del Twit This, Twitter también ofrece un buscador que permite buscar en cada momento qué se dice sobre un tema en concreto. Los resultados son un conjunto de comentarios hechos por diferentes usuarios donde sale la palabra de búsqueda indicada. Hay también el Tweet Beep, un servicio de alertas al correo electrónico de todos los micromissatges que escriben los usuarios que lo siguen o el Tweet Later para hacer que los micromissatges lleguen más tarde a los usuarios. El uso se ha extendido hasta el punto de que hay gobiernos como el de Australia que alientan la población a utilizar herramientas

como el Twitter o el Facebook en caso de alarmas de incendios o emergencias.

- Integración de sitios de redes sociales

  — Friendfeed
  Friendfeed es una herramienta que permite desde un mismo lugar agregar toda la actividad en línea: las fotos que subimos, los vídeos, los posts que se escriben, los eventos donde nos apuntamos, la música que escuchamos como favorita, los enlaces que guardamos, etc. todo lo que sea susceptible de hacerse mediante una aplicación en línea. A todo esto se le añade una capa social, con el que se puede seguir lo que hacen los demás usuarios y viceversa, filtrando las actividades que nos interesan y las que no.

- Ejemplos de sitios de redes sociales

  — Sitios de redes sociales: Facebook, Tuenti, etc.
  Los sitios de redes sociales se han popularizado muchísimo por ser herramientas que permiten mantener el contacto con los “amigos"que físicamente es difícil de mantener. Ha sido un fenómeno bastante generalizado en cuanto a edades y que ha afectado a todo el planeta. Los hay de genéricas (como Facebook o Tuenti) y especializadas. Entre las especializadas hay temáticas, como Pleiteando, red de personas relacionadas con el mundo de la justicia, de geográficas, como Migente, que incluye hispanos que viven en Estados Unidos; redes en que se comparten gustos musicales, como Last.fm, o videos, como YouTube. Lo que tienen en común todos estos sitios de redes sociales es que para registrarse el usuario crea el perfil digital. Últimamente, Facebook ofrece la posibilidad de personalizar el perfil de usuario, de manera que no aparezca una retahíla de números y letras sino una dirección URL más corta, más amigable, que contiene el nombre del usuario y que, por tanto, es más fácil de recordar.

  — Buscadores de identidades (Pipl.com, yasni.com o 123people.es)
  Se han creado también sistemas que funcionan como buscadores, en los que poniendo el nombre de la persona que nos interesa el sistema busca todas las identidades que tenga en la web, ya sean vídeos, sitios de redes sociales, blogs, etc. Hay que tener presente, sin embargo, que en los buscadores de entidades como los mencionados surge el problema del ruido en la recuperación de nombres y apellidos comunes, ya que a menudo no hay una correspondencia unívoca entre el nombre y la identidad.[6]

7. Riesgos

Uno de los problemas de la identidad digital es la posibilidad que tiene un solo individuo de generar una pluralidad de identidades, ya si bien es cierto que hay a quienes les conviene trabajar en la correcta construcción de su identidad

digital para adquirir más impulso o reconocimiento social o político, también lo es que pueden existir motivos por los cuales una persona desee permanecer en el anonimato que brinda internet, por distintos motivos, tales como robo-identidad-digital temas de seguridad, libertad de expresión, para ocultar o disfrazar los actos o consultas de información, o cuando simplemente se tenga el interés de que tales actos no afecten la identidad principal.

Es así que lo anterior puede representar un problema para las empresas, las autoridades o para quienes prestan servicios vía web, o cuando la contratación de los productos o servicios se realiza mediante estos medios, ya que es muy complicado saber quién es la persona que en realidad está realizando la transacción, quedando expuestos por ejemplo: a fraudes cometidos por el uso de identidades digitales falsas, los cuales en combinación con el uso de tarjetas de crédito clonadas o robadas, puede ser una herramienta muy peligrosa.

A diferencia de la identidad en el medio físico en la cual es más fácil identificar la persona que está realizando la operación, en el medio digital tenemos el problema de la falta de conexión entre una persona determinada y una identidad digital, tan incierto puede ser que al momento de cerrar la conexión la identidad digital puede dejar de existir.

La suplantación de identidad es otro de los problemas que afecta a una de las identidades parciales del individuo, es decir, se da una afectación a una de las cuentas o aplicaciones a las cuales tiene acceso el individuo, lo cual a su vez y dependiendo del grado de intromisión y del daño causado, puede llegar a cambiar en grado considerable la identidad digital del individuo.

Lo anterior puede ser realizado mediante distintas formas, entre ellas, el uso del nombre o usuario de la persona, se genere una identidad que ridiculice a la identidad original o se haga un uso no autorizado de la cuenta, pero al final tendremos como consecuencia la afectación a la privacidad, bienes, honor o reputación de una persona.

Otros de los problemas más comunes asociados a la identidad digital son las violaciones a los derechos la privacidad, los derechos autorales o daño reputacional en caso de empresas y personas, o sexting y bullying en caso de las personas, entre otras actividades que van deteriorando o violentando la identidad digital de una persona o empresa, llegando a grados en los que incluso se lleguen a afectar las relaciones personales y la vida íntima en el lado de la persona, o la imagen y reputación de una compañía.

La política actual de protección de datos supone que los usuarios deben aceptar explícitamente las condiciones de los servicios digitales a los que acceden, y que se responsabilizan de la veracidad de los datos que aportan, mientras que las empresas e instituciones que disponen de sistemas de recogida y gestión de datos

personales deben garantizar que el sitio cumple con los requisitos de protección y privacidad de los datos que reciben. citeriesg

Desde Kaspersky Lab aseguran que el robo de identidad es un problema creciente y propone una serie de consejos para evitar este tipo de amenazas:

- No almacenar datos financieros. Es cómodo tener almacenados los datos de tarjeta de crédito o la dirección de facturación en las tiendas online donde se suele comprar. No obstante, debido a las brechas de seguridad de estas páginas, es conveniente no hacerlo.
- Cuidado con las estafas digitales. Existen muchas formas de timos online. Algunos de ellos se reconocen fácilmente: como el email procedente de una familia real en África, la cual quiere compartir con nosotros millones de dólares. U otros más engañosos como las notificaciones para restablecer la contraseña de nuestra entidad bancaria. De todos modos, hay que ser cautelosos ante cualquier mensaje online que pida información personal o requiera la descarga de un archivo.
- Seguros. El robo de identidad se ha convertido en un riesgo que ya cubren las empresas aseguradoras, protegiéndote en caso de ser víctima de un ataque de este estilo.
- El riesgo de los dobles. Una de las formas con peores consecuencias del robo de identidad es crear una presencia online doble que haga creer a nuestro círculo que somos nosotros e intercambien información con alguien desconocido. Aunque se trate de una broma, este ataque puede dañar nuestra reputación. Para evitarlo, desde Kaspersky Lab recomiendan a los usuarios buscarse periódicamente en Google o Facebook para asegurarse que nadie se está haciendo pasar por nosotros. Si es éste el caso, se debe informar de dicho abuso en la red social pertinente e intentar cerrar el perfil cuanto antes.
- Rapidez. Si un usuario cree que ha sido víctima de un robo de identidad, tiene que actuar lo más rápido posible. Debe ponerse en contacto con el banco, proveedor de email o cualquier plataforma comprometida. Normalmente, los robos de identidad poseen motivaciones financieras y pueden tener un efecto devastador en la cuenta corriente.
- Usar contraseñas seguras. Los ataques contra los servicios en la nube como DropBox o LinkedIn han puesto en peligro la seguridad de millones de usuarios. No obstante, es posible ponerles un límite si se utilizan claves seguras y robustas. Lo cierto es que no es sencillo recordar una contraseña segura (larga combinación de letras, números y caracteres no alfanuméricos) por lo que la mejor opción es utilizar un gestor de contraseñas –password manager- que ofrecen las soluciones de seguridad de Kaspersky Lab. Además, es aconsejable cambiar dichos códigos con frecuencia, usar claves únicas para cada cuenta y tener una cuenta de correo electrónico solo para las finanzas online. [8]

8. Conclusión

Cada día se vuelve de mayor importancia la correcta gestión de la presencia en Internet y por tanto, la alfabetización digital se vuelve imprescindible ya que se vive en una sociedad conectada. Es importante conocer las tecnologías y la manera de utilizarlas para poder ser capaces de aprovechar al máximo los beneficios que se nos ofrece y también estar al tanto de las formas negativas en que nos pueden afectar.

La necesidad de poseer la habilidad de manejar nuestra identidad en la actualidad es evidente mas aún porque se conectan con nuestras identidades personales y nuestra reputación se pone en juego. Una mala reputación digital puede deformar nuestra imagen personal, intoxicar nuestras relaciones personales e incluso arruinar nuestras expectativas profesionales. Nuestros derechos y necesidades humanas básicas, dar a conocer, buscar, encontrar, transformar y distribuir información deben reconciliarse con nuestra igualdad de derechos y la necesidad de dejarnos solos. Tenemos derecho a decidir a retener, a permanecer en silencio, a resistir. Esto es lo que está en juego aquí: nuestra propia soberanía legítima sobre nuestras historias de vida, nuestras narrativas personales, nuestras comunicaciones e incluso nuestros propios recuerdos.

De forma general, es recomendable no aportar datos personales en la red y, en todo caso, brindarlos en los entornos más seguros posibles y directamente a personas conocidas, controlar nuestras configuraciones de privacidad y limitar nuestra presencia en la red.

Referencias

1. Identidad Digital y Reputación Online. Cómo gestionar tu presencia en Internet: http://www.voluntaddigital.com/blog/identidad-digital-y-reputacion-online-como-gestionar-tu-presencia-en-internet/
2. Digital Identity: What it is, why it matters and the impact it will have: http://indianexpress.com/article/technology/tech-news-technology/digital-identity-what-it-is-why-it-matters-and-the-impact-it-will-have/
3. Tu huella digital: http://www.internetsociety.org/es/tu-huella-digital
4. Online identity: is authenticity or anonymity more important?: https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity
5. How Google determined our right to be forgotten: https://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search
6. La gestión de la identidad digital: una nueva habilidad informacional y digital: http://bid.ub.edu/24/giones2.htm
7. Riesgos de la Identidad Digital: https://blogs.deusto.es/master-informatica/riesgos-de-la-identidad-digital/

8. Los peligros de la identidad digital: http://www.larazon.es/sociedad/tecnologia/los-peligros-de-la-identidad-digital-HF2645018#.Ttt1M3KCVNi3TyR