Big Data: el Valor de la Información Personal y la Privacidad

Big Data: the Value of Personal Information and Privacy

Carlos Fernando Arenas Fonseca
Tunja, Boyacá, Colombia
cafearfon@gmail.com

Recibido / Received: 23-05-16 – Aceptado / Accepted: 19-09-16

Resumen

El presente documento tiene como objetivo ilustrar el impacto que tiene Big Data y, en particular, el análisis de información a gran escala con respecto a la afectación de nuestra privacidad, y qué tanto valor se da a la información privada de los individuos actualmente. Adicionalmente, se pretende ilustrar que cada individuo acepta de manera ilimitada y libre, el uso de su información privada por terceros que la utilizan en su beneficio propio y de otros; y qué consideraciones se deben tener para restringir el uso que hagan estas compañías de la información personal y privada.

Palabras clave: Big Data, análisis de información, traza digital, privacidad.

Abstract

This document pretend to illustrate the impact of Big Data and in particular the analysis of large-scale information regarding the involvement of our privacy and that much value is given to the private information of individuals currently. Additionally it intended to illustrate that each individual accepts unlimited and freely use your private information by third parties who use it for their own benefit and others; and considerations should be taken to restrict the use they make these companies personal and private information.

Keywords: Big Data, information analysis, digital trace, privacy.

I. Introducción

En general, cuando se hace referencia a Big Data, existe la percepción que corresponde a la manipulación de la información que realizan las empresas de diferentes fuentes de información endógenas y exógenas de las organizaciones para darle un uso comercial y financiero mediante el impulso de sus productos y servicios a una población específica del mercado y, así, aumentar sus ventas y participación de mercados. Quizá este era el propósito inicial con el que fue concebido Big Data, pero en un mundo cada vez más interconectado y que demanda un flujo de datos continuo (en promedio, un individuo invierte 3,3 horas al día haciendo uso de internet [1]) ha elevado exponencialmente no solo los datos que

consumimos de la red sino los datos que generamos, ya que aplica en todos los aspectos de nuestra vida, haciendo que se vean expuestos en la red permitiendo que nuestra personalidad, preferencias e ideas pueden ser representadas como un dato.

Esto ha hecho que internet contenga más información de nosotros que la que conocemos, y de ahí la importancia y el valor que tiene nuestra información personal y privada depositada allí, por lo cual es muy posible que ni siquiera tengamos claro que representa para nuestras libertades y la expresión de nuestra personalidad el tener segura nuestra información más privada y valiosa. Sin siquiera darnos cuenta, toda acción, expresión, opinión o crítica que generemos en internet está siendo registrado, almacenado y monitoreado muy posiblemente sin nuestro conocimiento o permiso explícito, sin tener conocimiento del uso que terceros lleguen a hacer pues nuestras acciones en internet son nuestra carta de presentación ante el mundo y refleja aspectos tan importantes de nuestras vidas como el social, laboral, financiero, entre otros.

Es por este motivo que, en los años recientes, el alcance de Big Data ha tomado gran trascendencia, ya que no solo se utiliza a nivel comercial sino que ha tenido impacto en sectores como la medicina en el diagnóstico y tratamiento de enfermedades basados e información personal del paciente y sus familiares, llegando a buscar predecir tendencias de mercado, e inclinaciones sociales y políticas que pueden alterar el orden mundial y nuestra dinámica social como individuos formando tendencias. Las tendencias hacen que los seres humanos seamos proclives a inclinarnos a seguir, aceptar y actuar en pro de las mismas, ya que existe el fenómeno de masas mediante el cual tendemos a inclinarnos al pensamiento colectivo, aunque individualmente pensemos o creamos de otra manera.

Este artículo pretende ofrecer una visión de los alcances actuales de Big Data; los impactos y riesgos que este puede ocasionar en la población en general y en la información personal y privada de los individuos; el impacto que tienen nuestras acciones en internet y cómo estas pueden ser utilizadas para desencadenar consecuencias en la sociedad actual y cómo podemos reducir el efecto que pueden producir en nuestra forma de vida.

II. Big Data Y Su Impacto En El Mundo

Uno de los inventos del siglo XX que más impacto ha generado en la humanidad, ha sido Internet, ya que ha logrado traspasar los obstáculos de tiempo y distancia, brindando una ventana en tiempo real de lo que pasa en el mundo y cómo este cambia día a día gracias a su intervención en el pensamiento y conocimiento global. A su vez, Internet ha logrado proporcionar herramientas para que las ideas, emociones y pensamientos de todas las personas, sean accesibles solo con el hecho de acceder a un portal web o una aplicación. Dentro de este concepto, encontramos medios de comunicación masivos como los blogs, artículos periodísticos e incluso vídeoblogs los cuales tienen tanta difusión como los medios tradicionales de comunicación (radio, prensa escrita o televisión).

Adicional al impacto mediático global, Internet se ha vuelto el medio favorito para que las personas puedan comunicarse y expresarse con sus amigos y familiares, lo cual ha llevado a masificar el uso de herramientas como las redes sociales, en las cuales expresamos nuestras emociones y sentimientos; así como otras herramientas que permiten interacción instantánea por medio de nuestros dispositivos móviles con nuestros contactos de conocidos, amigos y familiares, tales como WhatsApp, Skype, SnapChat, entre otras.

Es tal la masificación de estos nuevos medios de comunicación, que en un solo día en Internet se generan más de 2,5 quintillones de bytes, lo cual equivale a más de 12,300 veces la cantidad de libros que han sido escritos en toda la historia [2] y se espera un crecimiento exponencial ya que solo para el año 2020 se espera generar 40 Zettabytes [3], lo cual representaría un crecimiento aproximado de 43 veces la cantidad de información que producimos actualmente. Continuamente se incorporan nuevas fuentes de información que exigen transmisión en tiempo real, lo cual hace algunos años no teníamos la posibilidad de tener al alcance: información de georreferenciación para establecer patrones de tráfi-

co y buscar la mejor ruta posible al instante, obtención continua de funciones vitales para monitorear remotamente el estado de salud de una persona e identificar síntomas de enfermedades existentes y alertar inmediatamente su ocurrencia, disponer de la posibilidad de comunicarse de manera instantánea con otra persona en cualquier parte del mundo con alta calidad de voz e imagen, entre otros; lo anterior sin contar con la explosión de información que generarán y consumirán los dispositivos que harán parte del internet de las cosas (IoT).

El problema que esto representa no es menor, ya se requiere todo un esquema que permita administrar la logística correspondiente a almacenar, clasificar, catalogar y estructurar información que está generándose en muchas fuentes diferentes y que requiere ser analizada en tiempos extremadamente rápidos, ya que lo que hoy es tendencia mañana puede que no lo sea. Es por esto que ha nacido como respuesta el análisis de información y datos, el cual tiene la finalidad principal de mostrar información relevante a las organizaciones de una forma consolidada para ayudar a la toma de decisiones mediante la explotación de un universo de datos específico en búsqueda de un objetivo particular, que es posible mediante la utilización de complejos algoritmos de búsqueda que permiten realizar búsquedas de patrones de información.

El análisis de información y datos no es como tal una ciencia nueva de la computación; desde que se ha establecido el proceso de recolección y persistencia de información, siempre se ha buscado explotar al máximo los usos que pueden darse de la misma. Es por esto que surgió la necesidad de mejorar la manera como se estructura la información para mejorar su análisis, por lo cual se pasó del uso de esquemas de datos indexados como lo han sido las bases de datos relacionales, pasando por catálogos en XML llegando a persistir información en métodos no estructurados para un fácil acceso e instantáneo como es la persistencia en la nube o en infraestructuras muy robustas que requieren grandes cantidades de memoria RAM para mantener toda la información disponible, ya que no se requiere acceder a discos duros para su consulta, concepto implementado por SAP HANA[4], demostrando un gran éxito a nivel empresarial. Uno de los pioneros con respecto a la explotación de información personal dentro de las organizaciones para el análisis de datos, es conocido como Business Intelligence, la cual mediante la aplicación de varios conceptos de análisis a bases de datos (DataMining, DataWareHousing, cubos de datos, etc.), permite obtener una visualización de la información de una manera consolidada y ejecutiva para la alta gerencia.

Lo que hoy busca, es expandir el alcance del análisis de la información a todas las fuentes de datos existentes; y ya que la mayoría de información producida por el ser humano persiste, por lo general, en el mismo gran repositorio centralizado (internet), esta tarea ha sido posible. Es por esto que ha nacido Big Data, el cual busca identificar en una gran cantidad de fuentes diferentes y con diferentes tipos de datos todas las correlaciones existentes entre las mismas y los patrones implícitos u ocultos que ofrecen los datos mediante la utilización de algoritmos complejos sobre un tópico particular, lo cual hace que se manejen volúmenes de datos extremadamente grandes en tiempos muy ajustados. Esto suena relativamente sencillo, pero realmente implica una logística conformada por un gran número de analistas de información, así como una plataforma tecnológica muy robusta que permita la obtención, almacenamiento y procesamiento de la información para obtener un resultado muy específico y orientado a satisfacer una serie de requisitos particulares.

Pero, con base en lo anterior, ¿cuál es la diferencia entre Business Intelligence y Big Data? Principalmente, es el ámbito y alcance de la información a analizar. Mientras que Business Intelligence es un proceso que se basa únicamente en la información existente en la organización; Big Data ofrece un universo más amplio en el cual se puede obtener información de fuentes externas que permita establecer la percepción fuera de la organización de temas relevantes, con el fin de poder dar respuesta a interrogantes que no la pueden tener con solo la información generada internamente. De hecho, Big Data permite complementar y establecer una vista más amplia del panorama de la organización internamente y exteriormente para mejorar el proceso de toma de decisiones organizacionales enfocadas,

entre otras, a la competitividad y su participación de mercado.

Dentro del análisis de información, los datos que son objeto de estudio son los generados en sitios web y redes sociales, tales como posts, tweets, likes, archivos publicados en redes sociales, entre otros; datos generados por humanos tienen como finalidad catalogar la interacción que existe entre usuarios y un sistema informático (registros de llamadas, correos, registros médicos electrónicos, información publicada en medios digitales e internet, fotos, videos, audios, etc.) y datos generados como parte de la interacción entre máquinas, la cual se mantiene por efecto de trazabilidad e integridad de las transacciones realizadas en internet (registro de transacciones, logs, registros de acceso, etc.) [5].

Según la forma como esta información persiste, se puede clasificar como información estructurada, semiestructurada y no estructurada [5]. La información estructurada es aquella que se encuentra almacenada, catalogada e indexada, lo cual permite una fácil identificación y acceso a la misma y, por lo general, está registrada en una base de datos o catálogo estructurado de datos. La información no estructurada corresponde a información que, por su naturaleza y origen, está en internet, pero no hace parte de una estructura de datos indexada que facilite su búsqueda. Por ejemplo, cuando se quiera establecer en una organización una búsqueda de una determinada información adicional a la búsqueda en las bases de datos e información catalogada existente se busque en otras fuentes como archivos de texto, diapositivas, hojas de cálculo, imágenes, videos, likes, tweets, entre otros. Por su parte, la información semiestructurada es aquella que, aunque no es almacenada en bases de datos, conserva cierta estructura mediante el seguimiento de pautas establecidas. Un gran ejemplo de esto son las páginas web, las cuales, aunque no tienen ningún tipo de estructura de información, tienen unos lineamientos establecidos para su presentación, como son los definidos por el lenguaje HTML.

Como se ha indicado, el universo de datos que conforman el análisis de información en Big Data es tan amplio y diverso, lo cual denota la complejidad que se requiere para estructurar dicha información, de forma que sea explotada adecuadamente y que el impacto que tiene cada uno de nuestras acciones en internet deja una huella que marcará nuestro presente y futuro, la cual es imborrable e inalterable, conocida como la traza digital.

III. Traza Digital

Al momento, más del 40 % de la población mundial posee una conexión a Internet [6], y se espera que para el 2017 los dispositivos móviles (Wi-Fi y redes celulares) generen el 68 % de todo el tráfico [7]. Esto representa un reto no solo a nivel de seguridad informática, sino a nivel de nuestra seguridad personal. Cada día, es más difícil no hacer parte de la ola digital, ya que nuestro estilo de vida está enmarcado por nuestra interacción con internet. Se considera que la probabilidad que una persona menor de 60 años que no haga parte de los servicios que ofrece internet ni que tenga redes sociales es muy remota, por lo que internet se ha transformado en la fuente de fenómenos sociales, culturales y laborales que han influido notablemente en la sociedad actual. La traza digital corresponde a cada una de las acciones que realizamos en el Internet y, por ende, todos los eventos que estas desencadenan: cada página a la que accedemos para buscar información de cualquier tipo, cada vez que abrimos nuestro correo electrónico, cada vez que actualizamos nuestras redes sociales, cuando realizamos búsquedas de bienes y servicios, todo esto está permanentemente registrado y monitoreado en sus sistemas.

Sin darnos cuenta, estamos proporcionando información de todos los ámbitos de nuestra vida, que puede ser utilizada para beneficio propio pero también para restringir nuestra propia privacidad. Cada vez que realizamos una búsqueda o publicamos un blog, post o un tweet acerca de nuestros pensamientos, sentimientos, creencias, estamos permitiendo establecer tendencias acerca de cuáles son nuestras ideologías, gustos y preferencias, lo cual puede ser capitalizado por un analista de información experto para establecer patrones de comportamiento, identificación de inclinaciones políticas e incluso religiosas que permiten elaborar un perfil personal que

puede ser analizado para identificar no solo aficiones y preferencias de todos los ámbitos de nuestra vida sino para poder establecer perfiles psicológicos de posibles terroristas antes que puedan realizar atentados, lo cual está en proceso de ser implementado por gobiernos de Estados Unidos y la Unión Europea [8]. Con la implementación de este modelo, se justificaría adjudicar a una persona el título de criminal, sociópata o terrorista sin haber cometido crimen alguno; solo identificar que cumple unas condiciones específicas al realizar una correlación de su información personal y privada. De entrada, esto corresponde a la presunción de un delito que no existe y, por lo tanto, no podría ser juzgado por un crimen que no ha cometido. De ser así, ¿cuáles serían las medidas que se podrían tomar contra el presunto futuro criminal? Cualquiera que sea la respuesta, va en contra de lo establecido en el artículo 11 de la declaración universal de los derechos humanos [9].

En este mundo globalizado, nuestra propia traza digital puede no solo afectarnos sino afectar a nuestro grupo digital, el cual está formado por todos aquellos que representan un vínculo establecido de manera digital desde cualquiera de nuestras fuentes de información personal, ya sean desde nuestros propios contactos telefónicos o de WhatsApp, pasando por nuestros contactos de correo electrónico y llegando a nuestros amigos virtuales en las redes sociales, ya que las mismas plataformas que utilizamos día a día y a las que hemos dado el control de nuestra información pueden establecer estas correlaciones de forma fácil y directa. De entrada, esto facilita la forma de interacción entre nuestros contactos, ya que reduce el esfuerzo de utilizar otras herramientas como el teléfono o SMS y facilita comunicación directa sin intermediarios. Es el caso de Facebook, el cual vinculará los números del teléfono móvil a su perfil gracias a que su perfil de WhatsApp le ofrecerá esta información, lo cual se autoriza mediante la actualización de condiciones de servicio que ha solicitado recientemente a todos sus usuarios, y que muy seguramente la gran mayoría ha aceptado sin tener esto en cuenta [10]. Con esto, lo que Facebook pretende es poseer la mayor cantidad de datos privados posibles de sus usuarios consolidando el poder de información que tiene de sus usuarios, puesto que no puede tener acceso completo a nuestros chats, imágenes y videos compartidos desde WhatsApp. Esto se da porque cada vez nuestro universo digital está más entrelazado entre sí; un ejemplo de esto son nuestros dispositivos móviles, cuando se van a usar por primera vez no se puede hacer uso de todos los aplicativos y servicios que este ofrece, debido que para esto se requiere por parte del dispositivo móvil ingresar con las credenciales de nuestra cuenta (para el caso de Android de Gmail, preferiblemente, o nuestra cuenta de usuario de Apple para el caso de IPhone).

Esto se hace para reestablecer en un nuevo dispositivo la configuración y aplicaciones que dispones con su perfil de usuario, ya que cuando se acepta el contrato de servicio que aparece en la configuración inicial del dispositivo y se acepta la opción de guardar copias de seguridad del mismo, estas opciones se ejecutan automáticamente. Sin embargo, la pregunta que queda es si realmente estos respaldos están siendo custodiados adecuadamente, y cuáles son los mecanismos de seguridad que utilizan para evitar que sean accedidos por terceros o delincuentes y, en caso de que esto llegue a ocurrir, cuál es el procedimiento para reclamar por el uso no autorizado que hacen de nuestra información.

Otra forma en que la privacidad de nuestra información es más vulnerada, proviene de nosotros mismos al aceptar consiente o inconscientemente los términos y condiciones de servicio para acceder a un servicio o aplicación que es “gratuita”, qué estamos aceptando la mayor parte de las ocasiones sin revisar en detalle las implicaciones y responsabilidades que como usuario está adquiriendo. Tal es el caso de Facebook, el cual en su contrato de servicio establece que el contenido publicado en su perfil aunque es de propiedad del usuario concede una licencia de no exclusividad para que Facebook lo utilice, licencia que finaliza una vez se ha eliminado el contenido de su perfil, lo cual permite que Facebook pueda hacer uso de nuestro contenido sin solicitar autorización al propietario mientras este contenido permanezca en el perfil del mismo. De igual manera, en este contrato se especifica que, aunque el contenido se haya eliminado del perfil, es posible que mantengan copias del mismo por un

tiempo no determinado, con lo cual podrían hacer uso ilimitado del mismo, ya que al ser eliminado por parte de nosotros como usuarios dejaría de ser de nuestra propiedad [11]. El caso de Twitter no es la excepción, incluso en sus condiciones de servicio, se especifica que con la aceptación del contrato se da consentimiento a la recolección y uso a la información provista por el usuario y que puede ser enviada a los Estados Unidos y/o a otros países para su almacenamiento, procesamiento y uso [12], impidiendo que el dueño del contenido sea realmente quien controle el alcance que tiene el mismo, ya que el poder de difusión lo tienen quienes nos proveen los medios para su publicación.

Incluso, existen casos en los cuales los individuos venden con total conocimiento su información privada: es el caso de la empresa Datacoup, la cual pagará un monto mensual no mayor a U$10 que se irá incrementando a medida que el usuario proporcione mayor cantidad de información personal privada, pasando por acceso a los contenidos publicados en redes sociales (Facebook, Twitter, Instagram, etc.), hasta compartir estados bancarios de tarjetas de crédito y cuentas bancarias, la cual Datacoup podrá utilizar y difundir de la forma que considere pertinente [13].

Con base en lo anterior, es claro que aunque desde su origen la información personal privada pertenece a nosotros como sus creadores, ha sido en gran parte nuestra responsabilidad que les hayamos brindado las herramientas a terceros de poseerla libremente sin que se cuestione el propósito para el cual se emplea, e incluso de manera consciente entregamos información personal privada a cambio de unos dólares sin considerar qué impacto tendrá en nuestra traza digital, ya que, como resultado de dicho análisis, se nos puede catalogar como parte de un nicho de mercado específico pero también con afinidad a una corriente política o ideología religiosa, lo cual puede definir desde la aceptación para pertenecer a determinados grupos sociales, pasando por apoyar o enfrentar determinados partidos políticos hasta estar en contra de religiones determinadas y quienes las practican. Esto representa un peligro para la sociedad actual y futura, ya que en vez de pertenecer a un modelo igualitario en el cual cada ser humano representa un mundo por sí mismo con sus propias creencias, valores y convicciones, lo que busca es segmentar y diferenciar a los seres humanos etiquetándolos por la información que genera y consume de internet, y en esto Big Data tiene y tendrá una gran relevancia, por lo cual toda nuestras actividades en internet han sido monitoreadas, ya que hacen parte de nuestra historia digital.

IV. Mecanismos Locales Y Globales De Protección A La Privacidad Y Seguridad De La Información

Hace unos años, cualquier individuo u organización que poseía información privada y personal de otros individuos, podía vender dichas bases de datos a terceros (cuyo uso y divulgación no necesariamente estaban autorizados) sin ningún control ni regulación ni imputación legal. Esta información, que inicialmente fue utilizada con fines de telemercadeo para identificar un nicho específico de clientes según su edad, sexo, estado laboral y financiero, entre otros, para productos y servicios específicos, se podía distribuir de manera abierta y con el conocimiento y permisibilidad de las autoridades, lo cual ocasionó hasta fraudes y eventos que afectaron el buen nombre de muchos individuos, por lo cual los gobiernos se han dado cuenta paulatinamente y se ha logrado la implementación de leyes de protección de datos privados y personales en la gran mayoría de países del mundo.

Uno de los pioneros en implementar este tipo de mecanismos, ha sido la Unión Europea, quienes bajo la directivas 95/46/CE [14] y 2002/58/CE [15] del Parlamento Europeo, establecen las herramientas para brindar seguridad en el tratamiento de los datos personales, así como la notificación de las violaciones de los datos personales a los usuarios y cómo garantizar la confidencialidad de las comunicaciones. De igual manera, prohíbe la entrega de información personal en las que el usuario no ha dado su consentimiento ni tiene conocimiento en todos los medios de comunicación digital, tales como correos electrónicos, mensajes de texto y demás sistemas de mensajería electrónica.

Para el caso particular de Colombia, es la conocida como la ley estatutaria 1581 de 2012[16], la cual especifica los mecanismos para la protección de datos personales, ya que todo individuo tiene el derecho constitucional de conocer, actualizar o rectificar toda información que se haya recogido en cualquier medio digital. Esta ley establece que, en caso de requerirse por un tercero datos de tipo privado de un usuario, este de dar su autorización escrita para que la empresa haga uso de los mismos y el usuario tiene el derecho de solicitar le notifiquen quién(es) hará(n) uso de esta información, así como que sus datos sean corregidos o actualizados en el caso que sea pertinente. Esta regulación aplica también para el registro de información privada obtenida para efectos comerciales, legales o profesionales que proporcionamos al vincularnos con una organización, corporación o grupo de individuo que la requiere para el registro en el sistema, ya que contiene información exógena que indirectamente pueda afectar toda la información pública del usuario con respecto a su perfil laboral, profesional, crediticio y legal.

Aunque estas medidas han mejorado notablemente el manejo que los terceros y corporaciones hacen de nuestra información personal y privada, surgen los siguientes interrogantes: ¿Quién controla que nuestra información, brindada con garantías de confidencialidad y con nuestra autorización, no esté siendo cedida o vendida a terceros? ¿Cómo se puede medir el efecto que pueden causar aquellos a quienes cedimos y autorizamos el uso de nuestra información cuando no se conocen los mecanismos de seguridad que estos emplean?

Un caso que ha tenido una amplia divulgación mundial, es el del portal de citas llamado Ashley Madison[17], portal web que promete encuentros amorosos con total discreción y confidencialidad, *hackers* han aprovechado vulnerabilidades en su seguridad y han accedido a su base de datos publicando en internet la información personal (nombres, teléfonos y correos electrónicos) y bancaria de todos los miembros del portal, afectando a millones de personas de todas las nacionalidades y condiciones sociales, generando desde divorcios hasta suicidios [18]. Sin embargo, la empresa dueña de este portal no ha realizado ninguna acción de reparación a los usuarios afectados y hoy sigue funcionando normalmente. ¿En este caso no deberían intervenir los organismos de control para restringir o cerrar definitivamente este portal? ¿Se han implementado mejoras en la seguridad del portal para prevenir que sus miembros no expongan su información personal a delincuentes que conocen las vulnerabilidades de seguridad de este portal? En este caso, se ha hecho muy poco con el fin de proteger la información personal y financiera de los usuarios de este portal y genera desconfianza con respecto al grado de protección que puede ofrecer las instituciones encargadas de proteger nuestra información personal, ya que se han presentado en diferentes portales de renombre, pasando por Google[19] hasta llegar al FBI [20] y otras entidades del gobierno de los Estados Unidos y a nivel global, por lo cual si no pueden restringir los ataques y protegerse a sí mismos, no se puede esperar que el individuo común sea protegido adecuadamente. Esto deja entrever que la seguridad de los datos privados y personales de los individuos depende, en gran medida, del valor que cada quien dé a su propia información y cómo protege su privacidad en nuestra sociedad actual.

V. El Valor De La Información Personal Y La Privacidad

Nuestra información personal y privada vale tanto como cada quien le dé su valor e importancia. En un mundo globalizado, es casi imposible que nuestra traza digital sea ninguna, ya que en cada ámbito de nuestra vida está internet, ya sea por la información que nosotros expongamos de nuestra vida como la que nuestros allegados exponen de cada uno de nosotros. Sin embargo, hay mecanismos para reducir la exposición de nuestra información personal y nuestra privacidad en internet:

- No publique en internet información privada sensible: muchas veces, sin darnos cuenta, podemos vernos afectados porque publicamos información privada sensible en internet, ya sea en nuestras redes sociales. Es importante que no se coloque información, tal como direcciones físicas, números de teléfono, números de documentos de

identidad, ya que esta información se puede utilizar por personas inescrupulosas en su propia contra.

- Deshabilite las opciones de localización de sus dispositivos móviles: la gran mayoría de dispositivos móviles cuentan con sistemas de localización mediante el uso del GPS que tienen incorporados. Por lo general, estas opciones vienen habilitadas y, sin darnos cuenta, estamos brindando información de nuestra ubicación pasada y actual, lo cual puede ser utilizado para establecer donde está ubicada nuestra vivienda, trabajo, cuáles son nuestras rutinas de desplazamiento, nuestros horarios de salida y llegada a nuestra vivienda, etc.

- Establezca con quién puede compartir su información privada: es conveniente limitar la cantidad de contactos o "amigos" con quien comparte información privada. Todas las aplicaciones tienen la posibilidad de limitar el alcance que tiene su información y quiénes podrán tener acceso a esta. Se recomienda que no acepte como parte de su grupo de amigos personas que no conozca personalmente o con quien no tenga contacto recientemente y esté seguro que el perfil de sus contactos sea verídico mediante la realización de preguntas cuya respuesta solo conozca usted o sus allegados.

- Evite publicar información escrita o audiovisual de sus propiedades: adicional a no publicar información como la dirección de sus propiedades, es importante no publicar en internet información como placas de vehículos o incluso imágenes o videos de sus propiedades ya que, de igual manera, puede ser utilizada para identificar su residencia o demás información privada que no quiere mostrar.

- Dar información personal a cambio de aplicaciones o servicios: casi todas las aplicaciones como redes sociales, acceso a portales y correo electrónico, entre otros, la requieren para tener acceso a sus servicios, los cuales son "gratuitos", se debe realizar un registro de datos personales. Es claro que ningún servicio en internet es gratuito, pues aunque no estemos realizando un pago por este, la mayoría de empresas obtienen ingresos o beneficios por la información diligenciada por sus usuarios. Es muy difícil obviar esto ya que es un requisito para tener acceso al sistema, por lo cual solo brinde la menor cantidad de información real posible y complete los campos requeridos con información falsa. Evite dar información de sus contactos o allegados, ya que es posible que si estos hacen parte del mismo servicio hayan brindado información real y puedan obtener parte de su información por correlación de información.

- Verifique las condiciones de los contratos de servicio: cuando se vincule a un aplicativo, portal o servicio, siempre verifique todas las condiciones de los términos del servicio que está tomando para identificar cuál va a ser el tratamiento que harán con su información personal y todos los archivos que usted obtenga y publique en el mismo, con el fin que tenga desde el inicio claridad de la finalidad que va a tener la información generada.

VI. CONCLUSIONES

Toda acción que se realice en internet es imborrable y hace parte de su traza digital, la cual define como individuo nuestra personalidad a través de internet con respecto a todos los ámbitos de nuestra vida, es por esto que debe tener presente que el uso que haga en la red puede marcar el perfil social, laboral e incluso económico que hoy en día es más relevante en nuestra sociedad actual.

La información personal y privada que produce un individuo, tiene un valor determinado que otros pueden explotar en su favor, ya que la información personal adquiere un mayor impacto en un mundo cada vez más interconectado y en el cual la privacidad es quizá el bien inmaterial más preciado.

Ningún servicio o aplicación de internet es gratuito, ya que al dar nuestra información personal estamos dándole el derecho que utilicen nuestros datos en su beneficio propio, sin tener ninguna manera de poder reclamar el destino que tenga nuestra información personal. Por lo general, al brindar datos personales en los formularios de registro no se especifica el uso que el servicio o aplicación realice con estos datos, así como tener la posibilidad de compartirlos con terceros sin ningún tipo de autorización del propietario de los datos.

Al afiliarse a un aplicativo o servicio de internet, es importante que se conozca las condiciones de servicio con respecto al uso de los datos personales y destino de todos los contenidos generados por el usuario, ya que se puede hacer uso indebido de los contenidos afectando la propiedad que el usuario tenga de los mismos, además, en algunas plataformas de redes sociales se publican contenidos que pueden ser distribuidos por la misma sin previa autorización de su creador.

Las opciones de geolocalización de sus dispositivos móviles, son utilizadas por las aplicaciones o servicios con el fin de ofrecer productos dependiendo de la ubicación del usuario o la posibilidad de conocer cuál de sus contactos está cerca a su posición. Sin embargo, esta información también puede ser utilizada por terceros en contra de su seguridad, ya que permite establecer rutinas de los usuarios basadas en sus patrones de movimiento.

REFERENCIAS

[1] Media (R)evolutions: Time spent online continues to rise. The World Bank public sphere, 2014. [Online]. Available: http://blogs.worldbank.org/publicsphere/media-revolutions-time-spent-online-continues-rise

[2] Google counts total number of books in the world. The Telegraph, 2010. [Online]. Available: http://www.telegraph.co.uk/technology/google/7930273/Google-counts-total-number-of-books-in-the-world.html

[3] Facts and Stats About The Big Data Industry. Cloud Tweaks, 2015. [Online]. Available: http://cloudtweaks.com/2015/03/surprising-facts-and-stats-about-the-big-data-industry/

[4] SAP HANA for real-time analytics. Big Data Made Simple, 2016. [Online]. Available: http://bigdata-madesimple.com/sap-hana-real-time-analytics-research-paper/

[5] M. Pérez Marqués, Big Data. Técnicas, herramientas y aplicaciones. AlfaOmega Grupo Editor, 2015.

[6] Internet users in the world. Internet Live Stats. 2016. [Online]. Available: http://www.internetlivestats.com/internet-users/

[7] Internet stats & facts for 2016. Hosting Facts, 2016. [Online]. Available: https://hostingfacts.com/internet-facts-stats-2016/

[8] Big Data en la lucha contra el terrorismoWhatsapp. Mundo Ejecutivo, 2015. [Online]. Available: http://mundoejecutivo.com.mx/tecnologia/2015/03/26/big-data-lucha-contra-terrorismo

[9] Declaración universal de los derechos humanos. Naciones Unidas, 1948. [Online]. Available: http://www.un.org/es/documents/udhr/

[10] Facebook tendrá acceso al número de teléfono de los usuarios de Whatsapp. El país, 2016. [Online]. Available: http://tecnologia.elpais.com/tecnologia/2016/08/25/actualidad/1472130602_996229.html

[11] Declaración de derechos y responsabilidades. Facebook, 2015. [Online]. Available: https://www.facebook.com/legal/terms/update

[12] Términos de uso y servicio. Twitter, 2016. [Online]. Available: http://www.twitterenespanol.net/terms_of_use.php

[13] Así funciona la compra-venta de tu información privada. MIT Technology Review,

2014. [Online]. Available: https://www.technologyreview.es/internet/46008/asi-funciona-la-compra-venta-de-tu-informacion/

[14] Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Parlamento Europeo, 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

[15] Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Parlamento Europeo, 2002. [Online]. Available: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al24120

[16] Ley estatutaria 1581. Congreso de la República de Colombia, 2012. [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[17] Portal de citas Ashley Madisson. Ruby Life Inc., 2016. [Online]. Available: https://www.ashleymadison.com/

[18] Dos suicidios estarían relacionados con 'hackeo' de Ashley Madison. El Tiempo, 2015. [Online]. Available: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/suicidio-de-usuarios-de-ashley-madison-portal-infiel/16279298

[19] Reportan el hackeo de casi cinco millones de cuentas de Google. Telám, 2014. [Online]. Available: http://www.telam.com.ar/notas/201409/77627-google-cuentas-hackeadas-gmail-rusia.html

[20] Anonymous cumplió: Hackeó la página del FBI. Ultima Hora, 2012. [Online]. Available: http://www.ultimahora.com/anonymous-cumplio-hackeo-la-pagina-del-fbi-n497204.html