Internet y la privacidad en 2020 (Y en el futuro)

Publicado el El Informatico - 6 de noviembre de 2020 -

Hoy me interesa escribir un artículo sobre un tema muy debatido en los últimos tiempos, que es el referente a la privacidad. Es un tema muy debatido por una buena razón, y es la monitorización constante en las redes por parte de empresas y gobiernos. El tema, no obstante, no es nuevo. Es un tema que lleva en la mesa desde mediados-finales de los 90, ya cuando internet empezaba a expandirse en algunos países y nació la web como la conocemos.

Un poco de historia...

Ya a mediados de los 90, todo el mundo sabía que se cocía algo importante con la llegada de la "web" a internet. Si bien, al principio, era algo primitiva. Las páginas web se desarrollaban en HTML en su primera versión, y se diseñaban más bien como "libros interactivos" con hipervínculos. Más adelante se expandiría sobre ese concepto con tecnologías como Macromedia Flash o Ecmascript (Hoy conocido como Javascript, o su versión de Microsoft, JScript), hasta evolucionar en un "matojo" de Javascript y especificaciones que hacen las cosas más complicadas de lo que deberían de ser.

Aunque la tecnología en aquél entonces era primitiva, era un nicho muy rico en información. La gente dedicaba páginas a sus familias, a sus mascotas, a sus equipos de fútbol favoritos, o simplemente a sus hobbies. Y como no, poco a poco las empresas comenzaron también a publicar contenido on-line. No tardamos mucho en poder empezar a realizar las primeras compras por internet y a visitar artículos sobre nuestros productos favoritos, así como a comentarlos en nuestras pequeñas páginas (antes incluso de que existiesen formalmente los blogs).

Las empresas que venden éstos productos o servicios se dieron cuenta muy rápidamente de que podían analizar toda ésta información para determinar los hábitos de consumo de una población en concreto, y poder así aumentar sus ventas orientando sus ofertas a dicha población. Así como mostrar publicidad personalizada en sus páginas web (La base de financiación de Google en sus

orígenes). Esta idea, aunque ya se realizaba desde hace muchos años en otros ámbitos fuera de internet, fue la que dio origen a lo que hoy llamamos el **big data**.

Por 'big data' entendemos la obtención de un cúmulo grande de información, y su procesamiento en piezas más pequeñas (pero con mayor significado) de información que nos pueden servir para obtener una visión global, mediante analítica de datos, de algo en concreto.

En la actualidad éstos datos pueden ser estadísticas de navegación sobre una página de comercio on-line tipo Amazon, en la que se incluye los productos que has estado mirando, cuánto tiempo le has dedicado a cada producto, el movimiento que has hecho con el cursor o el dedo sobre la página, la posición de la vista de la página y cuanto tiempo se ha permanecido en dicha posición, o en casos extremos se ha llegado incluso a usar la cámara del dispositivo del visitante para analizar la mirada y poder determinar donde se ha mirado y la expresión facial de la persona. Suena exagerado, pero es una realidad y muchas empresas, incluso Facebook, se han visto en los tribunales por éste tipo de prácticas.

Esos datos después se procesan y se convierten en datos más pequeños, con un significado mucho mayor. Por ejemplo, la relación entre todos los artículos que has visitado, lo que has comprado al final, cuáles son tus intereses en torno a esos productos y en qué productos podrías estar interesado (para ofrecerte recomendaciones), e incluso tu nivel de satisfacción y experiencia con la página. Todo el proceso está automatizado y se usan algoritmos de inteligencia artificial para su analítica.

Suena bastante inofensivo, ¿Verdad? Pero el agujero del conejo es bastante más profundo de lo que aparenta en la superficie.

Para la gente de a pié toda ésta información le resulta irrelevante. Y, si además eso mejora su experiencia como usuarios o clientes, mejor para ellos. ¿Verdad? Pero la información es más que eso. **La información es poder**. Es tal ese poder, que genera un interés muy muy elevado por parte de empresas, corporaciones, y otras entidades en esa información. **Es tal el interés, que se pagan sumas muy, muy elevadas por comprar datos y analíticas ya tratadas**. ¿Por qué? Pensadlo un poco.

Para un comercio o servicio, como ya he explicado, le supone la diferencia entre conseguir 10.000 ventas extra, o no conseguir ninguna, mediante anuncios orientados a compradores potenciales (targeted ads), sugerencias en comercios on-line, o campañas en las redes sociales. Para una página web supone tener una visión de los visitantes y sus tendencias de uso. Para un desarrollador de software (o como le gusta llamarlo ahora a la gente, "apps") supone tener una visión de las estadísticas de uso de su software. Para una entidad como el gobierno, le supone el poder

analizar los hábitos y las tendencias de sus ciudadanos, así como identificar amenazas potenciales (hablo de amenazas principalmente para ellos). Y no sólo eso, también les sirve para orientar sus campañas electorales e incluso llegar a convencer a gente para que les voten, aprovechándose de ese conocimiento.

Esto genera tal interés por esos datos, **que muchas empresas llegan a sobrepasar el límite de lo que es moralmente e incluso legalmente aceptable para hacerse con un pedazo de ese conocimiento**. Un ejemplo claro es el del escándalo entre Cambridge Analytica y Facebook, en 2016, donde se vendieron datos de millones de usuarios de Facebook a dicha compañía para poder ofrecerles estadísticas y apoyo a los partidos que hicieron campaña en dicho año. Y no creo que la campaña de éste año en EEUU (2020) haya sido muy distinta en ese ámbito.

Privacidad en redes sociales

Si eres usuario de redes sociales, o planeas hacerte usuario de ellas, ten clara una cosa: **olvídate de tu privacidad**.

Si te unes a una red social donde te obligan a usar un número de teléfono, estás firmando todos tus mensajes con nombre y apellidos. Y no importa que dicha plataforma te permita mostrar un nombre diferente y ocultar tu número de teléfono de cara al público, ya que en su base de datos les consta tu número. De modo que si una empresa indaga en tu perfil, van a saber que eres tú y van a saber todo lo que has estado diciendo, así como todos los memes que hayas posteado o tus fotos íntimas.

Si ésto te preocupa (que debería), entonces deberás borrar de inmediato tu perfil y no contribuir más en él. Probablemente ellos se queden con una copia de tus datos por un tiempo hasta que lo borren (a pesar de que la GDPR les obliga a borrar toda esa información si eres residente en Europa), pero al menos no les darás más escusas a las empresas para despedirte o no contratarte.

Pero si ésto no te preocupa en absoluto y decides seguir usando redes sociales, entonces deberás tener en cuenta que **todo lo que publiques en ellas (y en internet en general) es información pública, sin importar si la plataforma permite ocultar ese contenido o no**. Ya que aunque la ocultes al público, sigue estando accesible dentro de la plataforma. Recuerda el caso de Cambridge analytica y Facebook.

Privacidad en dispositivos inteligentes

Ya es algo común el uso de la etiqueta “inteligente” en cualquier dispositivo que se conecte a internet. Desde “teléfonos inteligentes” (smartphone), frigoríficos inteligentes, relojes (smartwatch), televisores… ¿Alguna vez os preguntáis por qué se les denomina inteligentes?

La etiqueta es una simple cuestión de *marketing*. Es ya algo habitual que un grupo de marketing asigne una palabra “amigable” para la población y el resto de empresas lo copien, como pasa con “la nube” (cloud), algoritmos de inteligencia artificial (AI y machine learning), etc. En la práctica, se le llama “smart” a todo lo que se conecte a internet para ofrecer al usuario algún tipo de servicio añadido o algún tipo de analítica.

Ahora bien, ¿realmente es necesario que un frigorífico se conecte a internet? Desde luego que parece conveniente que tu frigorífico sepa cuándo te falta de un producto determinado y sea capaz de encargar más cantidad de forma completamente automática. Pero ésto significa que **la empresa es capaz no sólo de conocer tus hábitos de consumo, sino de controlarlos**. ¿Para qué molestarse en elegir una marca o un producto distinto? Deja que un algoritmo se encargue de elegir por ti cuando lo crea más conveniente.

Lo mismo es aplicable para los “asistentes virtuales”, los cuales no sólo controlan tus hábitos cotidianos dentro de tu casa, sino que disponen de unos micrófonos con los que pueden escuchar constantemente todo lo que se oye en la casa. Si ésto no es un “caballo de trolla” en toda regla, no sé qué lo será.

Y ni qué decir de los teléfonos móviles modernos… ¡Todos tenemos uno en el bolsillo! Y todos tienen conectividad <x>G, GPS, bluetooth, micrófono y varias cámaras, así como un sinfín de “apps” llamando a casa constantemente y la posibilidad de además poder instalar malware en ellos. ¿Alguna vez te has parado a pensar por qué todas las compañías que fabrican teléfonos con Android, siempre traen una serie de aplicaciones que no puedes desinstalar y que a veces te las instalan a la fuerza mediante actualizaciones?

Mi regla de oro es que, si un producto dice ser “inteligente”, **desconfía**.

La privacidad y la seguridad

Tanto las empresas como los gobiernos van a camuflar sus actividades mediante un halo de conveniencia para la población. Por ejemplo, si ponen 400 cámaras CCTV a lo largo de la calle, dos en cada esquina, lo hacen con la idea de “protegernos frente a delincuentes”. Piénsalo, ¿Crees que a un ladrón le va a importar que haya 400 cámaras de seguridad en una calle? Cuando roban, ya van preparados con la idea de que hay cámaras grabando en el establecimiento. Por eso siempre van

encapuchados y actúan con rapidez.

Tal vez esas imágenes le puedan ayudar a las fuerzas del "orden" a capturar a los asaltantes en el futuro, pero eso no les impide cometer el delito. El establecimiento ya ha sido robado, aun delante de esas cámaras. Por ese motivo, **una vigilancia masiva nunca será un reemplazo adecuado para la seguridad ciudadana**. Es más, si conectaran esas cámaras a un sistema con inteligencia artificial y reconocimiento facial, entonces tendríamos un sistema de vigilancia masiva como en países como China. Lo cuál se puede convertir en un arma de doble filo para la ciudadanía.

¿Piensas que ésto es una exageración? Entonces te interesa conocer el experimento realizado en Valencia (España): Mercadona implanta el reconocimiento facial para detectar a personas con la entrada prohibida. Si bien a Mercadona puede que le vaya muy bien ésta tecnología para evitar que la gente que les ha robado entre de nuevo en sus tiendas, para que ésta funcione deben tener cámaras en cada esquina, procesando indiscriminadamente las caras de todas y cada una de las personas que entran en el establecimiento, sean delincuentes o no. Lo cuál puede que no sea del agrado de todo el mundo por razones que, a mi, me parecen lógicas.

Por supuesto, todas éstas prácticas se aplican por igual en internet. Cada día es más común ver noticias sobre gobiernos imponiendo leyes para poder monitorizar e incluso censurar las redes sociales. En España ya se han redactado sendos borradores, uno para una ley que pretende censurar los mensajes "de odio" de las redes sociales, y otra para censurar a los medios de información. Naturalmente que los mensajes que incitan al odio, sean de la naturaleza que sean, no tienen cabida en ningún sitio. Eso es indiscutible, y muchas redes sociales ya tienen normas estrictas contra éste tipo de contenido. Ahora bien, habrá que ver lo que el gobierno decide que es un mensaje de odio, y lo que no. Así como la aplicación de la ley que no será sencilla de aplicar. No tan conforme estoy con la medida para la "desinformación", ya que es una vulneración del derecho a la libertad de prensa y a la libertad de expresión, al tomar el gobierno la potestad de decidir qué es desinformación y qué no.

Si te interesa saber algo más sobre la vigilancia masiva en las redes, te interesará echarle un vistazo a éste artículo de la wikipedia, en el cuál se te quitarán las ganas de dormir.

La privacidad y el COVID-19

La situación tan peculiar que estamos viviendo en éste 2020 (y seguiremos viviendo durante todo 2021) ha generado una nueva cuestión en relación a la privacidad... "¿Y si pudiéramos gestionar mejor la pandemia controlando y monitorizando la

actividad de todas las personas?". La idea viene, como no, de China. Y sugiere controlar los movimientos de toda la población y sus contactos mediante conexión bluetooth. De este modo, se puede saber si has estado en contacto con un infectado y, de ser así, avisarte y ponerte en cuarentena.

Lo cierto es que todo puede ser útil y tener un lado bueno, pero en casos como éste, hay una palabra clave: **transparencia**.

Si por algún motivo se debe hacer uso de tecnologías de vigilancia masiva, se debe garantizar a la población que se respetan sus derechos y que se respetan las leyes, y se debe permitir siempre que la gente sea capaz, en todo momento, de verificar que ésto es así y de que se cumple con las legislaciones vigentes.

La información es poder

El problema que tiene la gente a la hora de comprender la importancia de la privacidad es que no comprenden la importancia de la información que dejan. Es algo normal, la gente está acostumbrada a cosas básicas que pueden manejar con las manos, oler con el olfato, saborear con la lengua... La gente es familiar con las cosas que pueden experimentar con sus sentidos. Pero no están tan familiarizadas con las cosas que NO se pueden sentir.

Por ese motivo, le pueden dar importancia a un teléfono móvil, una televisión inteligente, o un ordenador. Pero no así a la información que dejan, porque lo ven como algo trivial. ¿De qué le sirve a una empresa que conozca que yo, por ejemplo, bebo coca cola?

Un ejemplo de por qué esto importa está en **las estafas**. Hace un par de días me llamaron por teléfono y preguntaron por mi nombre, añadiendo al lado "titular de la línea de <nombre de la compañía telefónica>".

Esta es una estafa muy común, te mencionan el nombre de tu compañía telefónica de alguna manera (sin decir que son ellos) para que te sientas familiarizado/a con ellos, para después ofrecerte un "descuento" en tu linea telefónica. Si la aceptas, te cambiaran de compañía sin tu saberlo.

Pero para que ésto funcione, el estafador debe conocer además del nombre de la víctima y su número de teléfono, la compañía que tiene contratada. Sin ésta información, puede que aciertes o puede que no. En mi caso yo cambié de compañía hace un par de años, y el nombre de la compañía que me dieron fue el de mi antigua compañía telefónica. Con lo cuál automáticamente sabía que se trataba de una estafa (igualmente lo sabía porque no se habían identificado como de dicha compañía).

Estas estafas son muy comunes, y lo son gracias a que los estafadores ganan mucho dinero gracias a ellas. Y **la clave está en conocer a tu víctima para ganarte su confianza, algo que sólo se consigue si conoces a tu víctima**.

¿Debería de preocuparme por ésto?

Normalmente cuando hablo sobre privacidad a una persona, la respuesta suele ser, "¿Y por qué debería de preocuparme por ésto? ¡Yo no tengo nada que esconder!". A ésta pregunta la respondo siempre de la misma manera: "En tu casa tienes cortinas y persianas para tapar las ventanas, algo tendrás que esconder detrás de ellas". Porque todos tenemos cortinas y persianas en nuestras ventanas. Nos sirven para cuando queremos un momento de intimidad. Ello no quiere decir que estemos cocinando drogas detrás de esas cortinas. Es sólo que puede que en algún momento no queramos que nos vean desnudos o simplemente queramos un momento de intimidad para nosotros mientras leemos. **Tener un poco de dignidad**.

Entonces, ¿Deberías preocuparte por todo ésto? ¡Por supuesto! **TODOS tenemos algo que ocultar**. Seguramente si te pidiera tu número de la tarjeta de crédito o tu número de teléfono, me dirías que no me lo vas a dar. Tampoco importa lo buena persona que seas o creas que eres, todo el mundo tiene dos caras. Pero de cara al público, siempre nos ponemos una máscara. Y si nos quitan esa máscara, nos sentimos desnudos.

El problema de vulnerar nuestra privacidad es que **nos sentimos desnudos cuando lo hacen. Y por el mismo motivo que nadie aceptaría que nos desnudasen en mitad de la calle, tampoco podemos aceptar que lo hagan mientras navegamos por internet**. Por ese motivo, la privacidad debería de ser siempre, SIEMPRE, un derecho fundamental, un derecho humano. Es una simple cuestión de respeto.

Probablemente escuches en alguna ocasión la frase "Si no tienes nada que ocultar, no tienes nada que temer". Pero yo pienso que es más bien al revés. **Es cuando no te dejan tener intimidad cuando tienes algo que temer**.

ANTERIOR

Free Open Source Software (FOSS): ¿Qué es? ¿Es relevante?

SIGUIENTE

TOR: Encriptación de tráfico (Y por qué deberías de usarlo)

Buscar ...

Entradas Recientes

- Encriptación LUKS con CRYPTSETUP
- Se acabaron las bromas. A partir de ahora vas a estar constantemente vigilado en todas partes.
- Microsoft anuncia su nueva versión de su sistema operativo: Windows 11
- La historia de Internet en España
- Terminología moderna usada en tecnología digital
- Desactiva la ejecución de JavaScript de los archivos PDF, en Firefox y TOR browser.

Categorías

Actualidad | Android | Básicos | Ciberseguridad | Criptografía | Emulación / Virtualización | FOSS | Hacking | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS

Acerca de mi

Acerca de ElInformati.co