Rastreadores, Hackers y Falsificadores: la web actual no es segura

La Realidad del Rastreo Digital y la Vulnerabilidad de Nuestros Datos

¿Alguna vez te has preguntado quién está rastreando tus movimientos en línea? Desde que iniciamos sesión en nuestro navegador hasta que la cerramos, nuestras actividades son rastreadas y almacenadas por varias corporaciones como Google, Microsoft y Facebook. Cada clic, compra o mensaje que enviamos queda registrado bajo el control de estas corporaciones quienes venden nuestra información a las empresas que buscan vendernos sus productos y servicios. Aunque las grandes corporaciones que rastrean nuestra información parecen ser seguras, a menudo son víctimas de piratas informáticos llamados **Hackers**, lo que ha resultado en robos de identidad masivos. A veces, ni siquiera necesitan ser hackeadas para obtener nuestros datos; simplemente los venden al mejor postor. Nuestros datos personales se han convertido en una mercancía valiosa que se compra y vende en el mercado negro digital. Esto ha provocado la propagación de noticias falsas, que se difunden porque generan interés.

¿El resultado? **Capitalismo de Vigilancia**. Pero si es una empresa pública que debe responder ante sus accionistas, cuyo único parámetro para el éxito son sus ganancias trimestrales o el precio de las acciones, ¿qué hacer? Si el ADN de su empresa es un

subproducto de una cultura de ganancias por cualquier medio necesario, ¿cómo podemos esperar que cambie esto? Muchas personas se sienten cada vez más como si estuvieran bajo un microscopio digital que rastrea de forma rutinaria sus deseos más básicos y luego los enfoca para hacer que su cumplimiento sea más fácil, más eficiente y más efectivo, lo quieran o no.

Debido a que la gran mayoría de nuestros datos ahora son propiedad de terceros y están controlados por ellos, nos enfrentamos constantemente a amenazas de seguridad. El protocolo web HTTP está limitado en su alcance por lo cual solo puede conectar computadoras, documentos y medios. Dadas las limitaciones de su época, este protocolo no incluye estándares universales para cuentas de usuario, identidad de activos, seguridad, permisos o transacciones.

El incentivo para que las empresas capturen datos y los centralicen bajo su control para monetizarlos es claro. El problema es que cuanto más centralizada está la información, mayor es la tentación para los hackers. Los sistemas centralizados, por su propia naturaleza, son susceptibles de ser pirateados, corrompidos, alterados, adquiridos, arruinados o incluso destruidos.

Falsificadores y Noticias Falsas, El Monitoreo Digital y sus Implicaciones

Debido a que la web no fue diseñada con una base de datos compartida en mente, y debido a que no tiene inicio de sesión, no mantiene ningún registro, bitácora o "estado" de nuestra actividad. Pero a medida que navegamos por la web, compramos en línea, leemos publicaciones, chateamos con amigos, salimos a correr por la mañana o estacionamos nuestro automóvil por la noche, varias corporaciones rastrean y recopilan nuestra actividad física y digital y estos datos los almacenan en sus servidores.

Desafortunadamente, esto también ha llevado a la promoción de **noticias falsas** y otra información falsificada que la hacen pasar por artículos genuinos. La monetización de nuestro comportamiento en línea y fuera de línea en realidad promueve historias falsas sobre las verdaderas porque fomentan una mayor participación de los usuarios. La falsa rabia "vende". Todos hemos sido influenciados por noticias falsas de maneras que nos han impactado personal, profesional y políticamente. Como comunidad global, el impacto total aún no se comprende realmente.

Echemos un vistazo más de cerca a las características clave que faltan en la arquitectura web original y que faltan en las definiciones actuales de Web 3.0.

La Necesidad de una Infraestructura Web con Identidad y Autenticación Integradas.

Actualmente, los usuarios de la web deben autenticarse con cada uno de los proveedores de servicios para acceder al servicio de un proveedor. Esto requiere que los usuarios tengan cuentas separadas para diferentes modos de interacción: navegar, mandar y recibir correos electrónicos, comunicarse, compartir, comprar. Como resultado, todo el valor de los datos asociados con dicha cuenta es propiedad, están controlados y monetizados por terceros como Google y Microsoft. Este es el caso de casi todos los servicios en toda la Web.

Por otro lado, la Web carece de un navegador abierto, basado en un protocolo espacial estándar, al que todos los usuarios puedan acceder.

Hoy en día, la Web no proporciona una validación confiable en tiempo real de usuarios, activos y espacios, o su identidad, propiedad y permisos para diversas interacciones y transacciones. Debido a esto, el riesgo de hackers es significativo por que pueden hacerse pasar por una persona, sus agentes o avatares. Un hacker puede editar contenido de Realidad Aumentada (AR) en el mundo físico o cambiar el valor de un elemento en un mundo de Realidad Virtual (VR) para su propio beneficio.

Los hackers pueden cambiar la totalidad o una parte de una escena aumentada o virtual, eliminar, editar o cambiar la información crítica que se muestra, por ejemplo

en una planta nuclear, desfigurar o dañar entornos, mover objetos, tomar control de drones, vehículos o robots automatizados, o inyectar software o contenido inapropiado o incluso psicológicamente dañino. Todas estas instancias pueden ocurrir con objetos, contenido o personas, tanto virtuales como del mundo real.

Los incentivos económicos para monetizar la web mediante el seguimiento de nuestra actividad de navegación, relaciones sociales e historial de ubicaciones para vendernos mejor productos y servicios superan las implicaciones morales para nuestra sociedad.

El problema no radica únicamente en la búsqueda incesante de un dólar; sino en la naturaleza insidiosa de una especie de monitoreo o espionaje muy lucrativo que produce ganancias por el costo psicológico de dar click, político, social o ambiental. Esto es lo que sucede cuando la mano invisible del mercado es guiada silenciosamente por un "ojo que todo lo ve" que permanece ciego a los efectos que sus acciones tienen en el mundo que lo rodea.

Lo que lleva a otra pregunta: ¿Estamos aplicando correctamente la Digitalización? En un artículo de agosto de 2018 titulado "El hombre que creó la World Wide Web", en Vanity Fair, el fundador e inventor de la Web, Tim Berners-Lee dijo:

"Demostramos que la Web había fallado en lugar de servir a la humanidad, como se suponía que había hecho, y falló en muchos lugares". La creciente centralización de

la Web "terminó produciendo, sin una acción deliberada de las personas que diseñaron la plataforma, un fenómeno emergente a gran escala que es antihumano".

Tal vez por eso parece que la versión distópica de nuestro futuro es inminente. En el fondo sabemos que algo anda muy mal y podemos ver todas las señales que aparecen en nuestras pantallas y se filtran lentamente en nuestra vida diaria. Podemos sentir que una nueva era de la Web se nos acerca como un universo oculto que pronto romperá el velo de nuestra realidad actual. Y es ese sentimiento, el zumbido de fondo digital de la ansiedad, lo que nos lleva a una elección crítica.