OPINIÓN

El problema de un sistema social adicto a los datos III

Por Ernesto Ángeles · 18 de agosto de 2023 · 8 min de lectura



Suplantación y robo de identidad; acoso; manipulación política y económica; llamadas de números desconocidos para extorsionarte; discriminación automatizada. Todo lo anterior está asociado al mercado de los datos personales, sus malas prácticas y las formas en las que pueden afectar a la población, ya sea directa o indirectamente.

Desde que navegamos en Internet, usamos un celular, vamos al médico o entramos a algunos lugares, otorgamos el acceso a diversos datos asociados a cada uno de nosotros, tal como nombre, dirección, cuentas de redes sociales, actividad digital; entre muchos otros más. Es así como todos y cada uno de nosotros somos fuente de una gran cantidad de datos, cuya naturaleza es abierta y no excluyente, ya que nuestros datos pueden ser usados por cualquier actor y con diferentes fines, tanto altruistas como mal intencionados.

Entre los múltiples riesgos asociados al mal manejo de datos se pueden identificar dos áreas: problemas personales y problemas sociales, los primeros pueden incluir violaciones a la privacidad y filtración de información sensible; robo de identidad o suplantación de identidad; acoso y amenazas; discriminación; perfilado incorrecto; vulneraciones financieras; daño a la reputación y angustia emocional; amenazas a la seguridad personal; problemas familiares; pérdida del control de la vida digital; manipulación y dificultades legales.

Mientras que los riesgos comunales asociados a un mal manejo de datos pueden incluir: discriminación sistémica; ampliación de la desigualdad; pérdida de confianza en las instituciones; estigmatización y exclusión; dificultades para acceder a servicios; falta de representación y equidad; disminución de participación cívica; falta de

transparencia; manipulación; desconfianza interpersonal; dificultades de acceso al mercado laboral y a mejores servicios públicos; así como ataques a instituciones públicas.

Pese a que es habitual esperar que todo actor responsable de los datos haga un uso correcto y legal de éstos, la realidad muestra que es muy común que los datos sean manejados maliciosamente, que los pierdan o que se los roben, algo que es más perjudicial de lo que se cree, ya que hay muchos datos de nosotros que son muy difíciles de cambiar, sino que imposibles, tal como el nombre, fecha de nacimiento, preferencias, datos biométricos, etc. Por lo que, una vez extraviados, tales datos estarán disponibles para diversas partes, incluidos los actores maliciosos.

Debido a que actualmente el mal manejo de los datos parece ser una norma más que una excepción, existen una serie de ejemplos que no sólo abarcan la economía y el sector privado, sino que también se extienden a la política, las instituciones y el sector público, aquí un breve recuento de algunos escándalos:

Uno de las afectaciones más comunes en el mercado de datos es que sus responsables pierdan las bases de datos o que terceros actores accedan a ellas a través de un hackeo, entre estos casos hay ejemplos como el incidente de la tecnológica Yahoo en 2013, cuando la empresa sufrió el robo de datos de más de TRES MIL MILLONES de cuentas, la información robada incluía datos de las cuentas de usuarios como nombres, direcciones de correo electrónico, fechas de nacimiento, contraseñas cifradas y, en algunos casos, preguntas de seguridad con sus respuestas tanto cifradas como sin cifrar. Y tal como pasa en la industria tecnológica, este robo de datos no se supo hasta mucho tiempo después (en 2016) y bajo un complejo proceso de investigación, ya que los incidentes de seguridad digital usualmente se tratan con bastante secretismo, sobre todo en la industria privada.

Otro caso aún más escandaloso fue el de Ashley Madison, una aplicación de citas principalmente para hombres casados, la cual sufrió un hackeo en 2015 y cuyos atacantes publicaron la información de más de 32 millones de usuarios; los datos hackeados incluían nombres, cuentas de correo electrónico, ubicación, fantasías sexuales de usuarios, fotos de desnudos y datos bancarios. Lo interesante de este caso fue que los datos no fueron resguardados por los atacantes, sino que, al contrario, fueron puestos a disposición de internet en general, lo que desencadenó una intensiva búsqueda de nombre de clientes de la aplicación (ya que se trataban de hombres casados), lo que pudo desencadenar actos de chantaje y amenazas.

El robo de datos en las empresas es un riesgo para sus clientes, ya que entre los datos perdidos puede haber información sensible que ponga en peligro las finanzas personales, la reputación, la salud y hasta la propia vida de las personas. Sin embargo, el hackeo de bases de datos no sólo ocurre con las empresas, sino que también incluye gobiernos e instituciones públicas, lo que no sólo pone en entredicho el bienestar personal, sino que también hace peligrar el funcionamiento de la vida pública, los servicios y el país en general.

Uno de los casos más sensibles y sonados ha sido la pérdida de datos del Instituto Nacional Electoral (INE), los cuales cuentan con un amplio historial de mal manejo de datos; el primero en 2016, cuando se supo que, tras haber facilitado una serie de memorias USB con las bases de datos del padrón electoral a los partidos políticos, Movimiento Ciudadano hizo un pésimo manejo de datos y recibió un ataque cibernético, lo que resultó en el acceso ilegal a 94.4 millones de registros que podían descargarse de los servidores de Amazon; entre los datos que contenían las bases estaban nombre, dirección completa, fecha de nacimiento, los apellidos de la madre y el padre, ocupación y el número de la credencial para votar. El segundo escándalo del mal manejo de datos asociados al INE sucedió en 2021, cuando Hudson Rock, una empresa de inteligencia sobre ciberdelitos, dio a conocer que encontraron en internet la venta de una base de datos con 91 millones de registros personales del INE.

Asimismo, el INE no es la única institución nacional afectada por un mal manejo de datos, tan sólo recordar el infame hackeo de Guacamaya Leaks, un grupo de hackers que robó información a la SEDENA, entre la que se encontraba el estado de salud del presidente Andrés Manuel López Obrador; otras instituciones que han sufrido robo de datos son: Infonavit, PEMEX, tribunales locales y federales y más.

Sin embargo, el mal manejo de datos no sólo incluye hackeos, robos y pérdidas, sino también está asociado a malas prácticas, abuso de poder y engaños, tal como sucedió en 2018 cuando se dio a conocer que la empresa británica de consultoría política, Cambridge Analytica, había obtenido indebidamente la información personal de alrededor de 87 millones de usuarios de Facebook por medio de una aplicación de prueba de personalidad, en donde los usuarios de la app no sólo dieron el acceso a sus datos, sino que también incluía el acceso a los datos de amigos y contactos en Facebook. El problema no sólo consistió en permitir el acceso a datos, sino que éstos fueron utilizados por Cambridge Analytica para generar contenido político a la medida, lo que les brindaba la posibilidad de manipular a los votantes para que favorecieran las necesidades políticas de sus clientes. Sobra decir que esta firma fue contratada en diferentes países alrededor del mundo, incluido México, en donde fueron contratados por nada menos que el Partido Revolucionario Institucional (PRI).

Otro caso pernicioso del uso de datos en contra de la población se dio con las aplicaciones de rastreo de COVID-19 en medio de la pandemia, las cuales no sólo llevaron a diversos casos de discriminación, exclusión y profundización de la desigualdad, sino que también muchos de los datos recabados terminaron en servidores e infraestructuras desconocidas; sin mencionar el recabo de datos no consensuado.

Otros casos más graves y dramáticos son cuando los datos se usan para difundir información falsa e identificar grupos sociales con el fin de excluirlos, dañarlos o asesinarlos, tal como sucedió en Myanmar en 2017, cuando el uso de Facebook fue central para perseguir a la minoría musulmana Rohingya, lo que se tradujo en el asesinato de más de mil personas y el desplazamiento de cientos de miles más. Estas tensiones étnicas no sólo han sucedido en Myanmar, sino que también la India ha sufrido fenómenos parecidos en 2020, en donde de nuevo las redes sociales (específicamente Facebook) sirvieron de herramienta de propaganda, incitación a la violencia e identificación de “enemigos”.

En conclusión: los casos expuestos en este artículo subrayan la importancia de reconocer que el mal manejo de datos no es simplemente una cuestión técnica, sino un problema profundamente arraigado en la ética y los valores sociales. La tecnología avanza a pasos agigantados, pero debemos asegurarnos de que nuestro avance sea acompañado por una reflexión crítica sobre cómo se utilizan los datos y cómo se protegen los derechos humanos, así como medidas para disminuir la desigualdad de capacidades de poder entre las empresas, el Estado y la sociedad. Sin embargo, tampoco hay que olvidar que la responsabilidad de atender este desafío también recae en todos nosotros, como ciudadanos informados y agentes del cambio.

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/opinion/el-problema-de-un-sistema-social-adicto-a-los-datos-iii
Descargado el 21 de noviembre de 2026.