¿Qué es la usurpación de identidad?

Dr. Alberto E. Nava Garcés*
Abogado penalista, investigador del Instituto Nacional de Ciencias Penales y miembro del Sistema Nacional de Investigadores (CONACYT)
iusnava@yahoo.com.mx

Síntesis

Este es el delito informático de más rápido crecimiento en el mundo que se castiga con una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días de multa, según la legislación penal para la CDMX. Para los bancos mexicanos, esto genera una pérdida de más de 261 mil millones de pesos al cierre de 2015 y para 2016, 2017 y 2018 va en aumento.

Resulta ya un lugar común referirse a los datos como el petróleo del siglo XXI. Para las generaciones pasadas los datos personales no parecen tener una mayor relevancia más allá de establecer características singulares que distinguen a una persona de otra, y para las futuras generaciones habrá que explicarles qué significaba el petróleo en el siglo XX. Pero ¿realmente tenemos que preocuparnos por cuidar nuestros datos?

Hoy en día existe la alta posibilidad de que llegue al domicilio una tarjeta de crédito no solicitada o diversa correspondencia que, si bien está dirigida al habitante de un domicilio, no deja de inquietar cómo ocurrió, en qué momento las empresas procesaron información para hacer llegar sus mensajes. Lo mismo ocurre con los usuarios de la red, cuando descubren que la publicidad (ADS) pareciera estar pensada en sus necesidades. Lo cual es cierto. El uso, las búsquedas, el tiempo que uno se detiene en las cosas que llaman la atención, las páginas abiertas, entre otros hábitos, forman una bitácora que, tanto las redes sociales (ver anexo 1) como los buscadores en Internet comparten para una explotación comercial (de ello dan cuenta los avisos de privacidad y contratos de uso, cuyas cláusulas pasamos inmediatamente, motivados por la ansiedad de iniciar la aplicación o entrar a la red) (ver anexo 2).

Los usuarios, por diversas razones, depositamos ingentes cantidades de datos personales, entre otras, las siguientes:

- Edad.
- Domicilio.
- Estado civil.
- Teléfonos.
- Ingresos.
- Lugar de trabajo.

- Dependientes económicos.
- Número de cédula.
- Número de licencia.
- Número de pasaporte.
- Número de credencial para votar.
- CURP.
- Números de tarjetas de crédito.
- NIP.
- Fechas de vencimiento.
- Número de seguridad social.
- Placas de vehículos.
- Claves catastrales.
- Predio.
- Identificador de contrato telefónico.
- Contrato de cable.
- Contraseñas.

Con estos datos estamos dotando a quien los recibe de una información que puede ser utilizada para cualquier fin.

¿Cuánto cuesta el robo de identidad?

Rouchón lo explica de este modo: "Para los bancos mexicanos, esto genera una pérdida de más de 261 mil millones de pesos, al cierre de 2015; y va aumentando en 2016, 2017 y 2018."[1]

Por otro lado, Raúl Cervantes cita:

> Para Luciano Salellas, el robo o suplantación de identidad es el delito informático de más rápido crecimiento en el mundo. Conocido también como *impersonation*, se entiende como suplantación de personalidad o identidad a quien funge ser una persona que no es. El caso más común es el robo o la utilización de tarjetas de crédito y documentos de terceros.[2]

Es el mismo Raúl Cervantes, quien clasifica al robo de identidad según su origen:

1) *Phishing* (solicitar información mediante correos falsos) es la duplicación de una página web para que el visitante crea que se encuentra en el portal original en lugar de uno duplicado. [...]

2) *Tabjacking*. Este tipo de ataque es conocido con este término y básicamente consiste en una página que, luego de un tiempo de inactividad, es reemplazada por otra que puede verse como la original, por eso es tan peligroso como cualquier otro *phishing*. [...]

3) *Pharming* (robo de información mediante el uso de páginas falsas). Es una nueva modalidad de fraude *on line* que consiste en suplantar el sistema de resolución de nombres de dominio (Domain Name Server o DNS) para conducir al usuario a una página web falsa. Aunque es una amenaza creciente y peligrosa, la solución está en la prevención y en un antivirus eficaz.

   Cuando un usuario teclea una dirección en su navegador, esta debe ser convertida a una dirección de protocolo de Internet numérica (IP). Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS, en los que se almacenan tablas con las direcciones IP de cada nombre de dominio. [...]

4) Spam y spyware (archivos malignos dentro de correos electrónicos). El spam son mensajes no solicitados y enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es por correo electrónico. Otras tecnologías de Internet que han sido objeto de spam incluyen grupos de noticias, motores de búsqueda y blogs. El spam puede tener también como objetivo los celulares y los sistemas de mensajería instantánea.[3]

   Por su parte, el spyware es un software que recopila información de una computadora y después la transmite a una entidad externa sin el conocimiento o el consentimiento del propietario. Un spyware típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha la computadora (utiliza el CPU y la memoria RAM, reduciendo así la estabilidad) y funciona controlando todo el tiempo el uso que se hace de Internet y mostrando anuncios relacionados.[4]

5) Compras por Internet. Los ladrones de identidad también pueden obtener la información de las tarjetas de crédito con las compras que el usuario efectúe en tiendas, por teléfono o Internet. Por ejemplo, la información de la tarjeta de crédito que proporciona el usuario durante una compra, en persona o por teléfono, puede utilizarse indebidamente para realizar cargos no autorizados en su cuenta.[5]

En México, la legislación penal no ha atacado el problema de manera homogénea, pero podemos encontrar algo al respecto en el artículo 211 Bis del Código Penal para el Distrito Federal (es curioso que siga manteniendo la denominación anterior de la Ciudad de México), cuyo texto señala:

> **Artículo 211 Bis.** Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otor-

Para los bancos mexicanos, **el robo de identidad genera una pérdida de más de 261 mil millones de pesos**, al cierre de 2015; y va aumentando en 2016, 2017 y 2018

> gue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días de multa.
>
> Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.

Edgar Hoover, antiguo jefe del FBI enseñaba a sus agentes que una buena investigación podía comenzar revisando la basura. Ahí podrían encontrase indicios sobre las costumbres del sujeto a investigar: sus llamadas, hábitos alimenticios, padecimientos más comunes, etcétera.

De igual modo, quienes roban la identidad lo pueden hacer desde un trabajo aparentemente inocuo; por ejemplo, un encuestador que solicita no solo que la persona describa alguna preferencia, sino además solicitándole alguna identificación o en los casos más comunes, hay quienes revisan la basura en busca de datos. Así que la próxima vez que pretenda tirar un estado de cuenta a la basura, piense en cuántos datos contiene y el mal uso que puede hacerse de ellos.

En el ámbito digital, Nico Sell ha publicado algunos consejos para la destrucción de datos y mantener comunicaciones seguras:

1. Afirma que es necesario desinformar a las redes sociales, por ejemplo, Facebook, respecto a datos como la fecha de nacimiento.

2. Debes tener cuidado con las personas y los sitios que te piden información. ¿Por qué necesitan mi número de Seguridad Social? ¿Por qué necesitan mis señas?

3. Hay que acabar con la geolocalización. Aplicaciones como Twitter, Instagram y Foursquare, que piden información sobre la ubicación del usuario, pueden ser utilizadas para obtener información personal mediante la ingeniería social o incluso para averiguar el mejor momento para robar una casa.

4. Hay que leer los tediosos acuerdos de privacidad.

5. No confíe en ninguna aplicación médica. Se refiere al número de datos que hay que proporcionar y lo delicado de su contenido.[6]

Los datos son muy importantes, pues la suma de ellos implica información. La información personal da lugar a un uso indebido, pero lo más importante es la prevención.

Anexo 1

Somini Sengupta señala: "SAN FRANCISCO– La página en Facebook del Hospital Gaston Memorial, en Gastonia, Carolina del Norte, ofrece una receta de ensalada de pollo para fomentar la alimentación saludable, así como tips para evitar lesiones al hacer ejercicio.

Pero, en octubre surgió otra página Facebook del nosocomio. Ésta criticaba al presidente Obama y su ley de salud. Reunió rápidamente a cientos de seguidores y las diatribas anti-Obama recibieron menciones 'me gusta'. Los empleados del hospital recurrieron a su verdadera página en Facebook para controlar los daños. 'Ofrecemos disculpas por cualquier confusión', expresaron el 8 de octubre, 'y agradecemos el apoyo de nuestros seguidores'.

La página espuria desapareció 11 días después, tan misteriosamente como había aparecido.

La falsificación es omnipresente en internet. Twitter, que permite el uso de seudónimos, está repleto de falsos seguidores y ha sido usado para propagar rumores falsos. Las reseñas falsas son un problema constante en los sitios de consumidores.

Para Facebook, el más grande de los sitios sociales, plantea un problema especialmente álgido porque pone en entredicho su premisa básica. Facebook ha buscado distinguirse como un lugar de identidad real en internet. Como le dice la compañía a sus usuarios: 'Facebook es una comunidad donde la gente emplea su identidad real'.

Menciones 'me gusta' fraudulentas dañan la confianza de los anunciantes, quienes quieren clics de gente

real a la que pueden venderles y con los que Facebook cuenta para ganar dinero.

Facebook recientemente intensificó sus esfuerzos para erradicar la falsificación en el sitio.

Falsos perfiles resultan bastante sencillos de crear; cientos de ellos pueden aparecer de forma simultánea, a veces con la ayuda de robots y, a menudo, convencen a usuarios de volverse sus amigos en un intento por diseminar software malicioso. Amigos de Facebook y menciones 'me gusta' falsos se venden por internet a las personas deseosas de mejorar su imagen. Vales de comida, gadgets falsos pueden aparecer en los 'muros' de Facebook, con el fin de engañar a víctimas involuntarias para que revelen sus datos personales.

Joe Sullivan, encargado de la seguridad en Facebook, indicó que la compañía cuenta con un nuevo sistema automático para purgar las menciones 'me gusta' falsas.

Sullivan explicó que se activan alarmas si un usuario envía cientos de solicitudes de amistad al mismo tiempo, o manda una liga a un sitio que se sabe contiene un virus. Aquellos sospechosos de ser falsos reciben advertencias y se les puede suspender la cuenta.

En el otoño, Facebook anunció asociaciones con compañías de antivirus. Los usuarios pueden descargar cobertura antivirus gratuita o pagada para protegerse de software malicioso.

La nueva agresividad del sitio hacia los 'me gusta' falsos se volvió perceptible en septiembre, cuando páginas de marcas comerciales empezaron a ver su número en seguidores súbitamente.

Los usuarios falsos y sus comentarios tendrán que ser contrarrestados de forma agresiva si Facebook quiere ampliar su función de búsqueda, afirmó Shuman Ghosemajumder, cuya compañía de arranque, Shape Security, se enfoca en falsificaciones automatizadas en internet. Si un usuario busca una laptop, por ejemplo, Facebook tiene que asegurarse de que pueda confiar en los resultados obtenidos.

Sin embargo, la ubicuidad de Facebook vuelve inevitable que dichos resultados conlleven una medida de falsedad.

Colleen Callahan, de 25 años, estaba en su último año de carrera universitaria cuando empezó a sentirse nerviosa por las fotos de fiestas que un eventual jefe podría encontrar en su cuenta de Facebook. 'No habría problema si la gente las viera, pero no quería que las interpretaran erróneamente', explicó. Entonces se convirtió en Colleen Skisalot. Aún emplea el nombre, aunque ya consiguió trabajo en una agencia de publicidad de Boston, de la que algunos se anuncian en Facebook. ("Identidades falsas agobian a Facebook", Reforma, sábado 8 de diciembre de 2012, Sup. The New York Times, p. 6).

Anexo 2

Joel Rouchón, en su conferencia magistral impartida en 2019 en el INACIPE señaló: "En México, la Constitución Política de los Estados Unidos Mexicanos de 1917 fue modificada el 4 de junio de 2014, sumando a la misma un decreto por el que se adiciona el artículo 4°, el cual fue publicado en el Diario Oficial de la Federación, con fecha del 17 de junio de 2014. En este se asienta lo siguiente:

Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento. Los elementos mínimos que deben figurar en esta acta de nacimiento son nombre, apellidos, fecha de nacimiento, el sexo, nacionalidad y el nombre de los padres.

A pesar de todas las medidas recientes de seguridad, es del conocimiento público que muchos países en el mundo todavía no tienen un registro civil actualizado. De hecho, en lugares alejados de algunos países en vía de desarrollo, muchas personas no han sido declaradas, ni registradas y tampoco tienen ninguna identificación.

Tampoco existen en estos países controles de la población; es muy fácil obtener un documento de identidad por medio de la corrupción y la falsificación de los soportes. Es posible hacerlo porque el Estado no invierte en la seguridad de dichos soportes.

La seguridad actual de la identidad y de la propiedad ligada a ella pasa por la perfección continua de la seguridad de los documentos de identidad. Ejemplo de esto es el nuevo código de barras tridimensional, que se comprueba con un lector o con un teléfono celular, cuando este contiene la aplicación idónea. Se trata de una herramienta muy perfeccionada que utiliza dos niveles de control (3D) cuando un lector de códigos de barras, o un escáner de códigos QR Utilizan únicamente la impresión en plano."

* Autor de los libros *Delitos Informáticos* (Porrúa) y *Delitos Electrónicos. Casos de autoría y participación* (Tirant lo Blanch – INACIPE).

1 Rouchón, conferencia magistral, INACIPE, 2019.

2 Luciano Salellas, "Robo de identidad". Disponible en http://www.cabinas.net/informatica/robo-de-identidad.asp consultado el 30 de agosto de 2010. Citado por Raúl Cervantes Andrade, "Robo de identidad" en ROQUE DÍAZ, JOSÉ RODRIGO. *Delitos de cuello blanco*, México: INACIPE, 2011, p. 111.

3 Véase http://www.descargar-antivirus-gratis.com/spam.php

4 Para más información visite las páginas: http://www.masadelante.coo/faqs/que-es-spyware; http://www.descargar-antivirus-gratis.com/spyware.php y http://es.wikipedia.org/wiki/Programa_esp%C3%Ada, entre otras.

5 Cervantes Andrade, *Op. cit.*, p. 112 – 114.

6 Texto completo en: http://actualidad.rt.com/sociedad/view/133269-consejos-privacidad-hacker-robo-datos