La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen

Abog. Marcelo G. I. Temperini[1] A.I.A. Maximiliano Macedo[2]

Abstract. Año tras año, sigue aumentando la cantidad de usuarios que se suman a las nuevas tecnologías, en cualquier de sus distintas alternativas, entre ellas y quizás más populares: las Redes Sociales. Según distintos estudios, Facebook sigue liderando el ranking de usuarios que usan sitios de redes sociales. El presente trabajo pretende hacer foco sobre la situación de los perfiles falsos existentes en la Red Social Facebook, precisamente por ser reconocida como aquella de mayor utilización, tanto en Argentina como a nivel mundial. En el mundo del cibercrimen, son los perfiles falsos en Facebook una herramienta de uso cotidiano por parte de aquellas personas que realizan un daño, es decir, son en muchos casos estos perfiles el medio a través del cuál se cometen delitos como injurias, extorsiones, amenazas, estafas y en los peores casos, corrupción de menores y grooming. Será entonces el objeto primario de estudio del presente trabajo, el análisis del fenómeno de los perfiles falsos existentes en la Red Social Facebook y como objeto secundario, se analizará la relación existente entre los perfiles falsos y el mundo del cibercrimen.ç

Keywords: delitos informáticos, seguridad informática, identidad digital

Abstract: The amount of new technology's users keeps growing year after year, on each of its multiple branches, among their most popular are: Social Networks. Acording to several studies, Facebook keeps leading the ranking of social network users. The present work intends to focus on the issue of fake profiles on the social network known as Facebook, known for being the one of primary use, both in Argentina and worldwide. In the world of Cybercrime, fake profiles are a common, everyday tool for people who seek to cause some kind of harm, this meaning, these profiles are in many cases the medium through which many crimes are commited, such as obloquies, black-mailing, threats, frauds and in worse cases, minor corruption of minors and child grooming. As such, the main focus of the present work will be the analysis of the phenomena of fake profiles existing on the Social Network known as

1 Abogado (UNL). Doctorando CONICET con especialización en Delitos Informáticos. Analista de Seguridad y Vulnerabilidad en Redes. Socio Fundador de AsegurarTe – Consultora en Seguridad de la Información. Contacto: mtemperini@asegurarte.com.ar

2 Analista en Informática Aplicada (UNL). Socio Fundador de AsegurarTe – Consultora en Seguridad de la Información. Contacto: mmacedo@asegurarte.com.ar

Facebook and, as a secundary study, an analysis on the existing relationship between fake profiles and the world of cybercrime.

Keywords: cybercrime, information security, digital identity

Introducción

Año tras año, sigue aumentando la cantidad de usuarios que se suman a las nuevas tecnologías, en cualquier de sus distintas alternativas, entre ellas y quizás más populares: las Redes Sociales. Según un estudio del PEW Research Center [1], Facebook sigue liderando el ranking de usuarios que usan redes sociales.

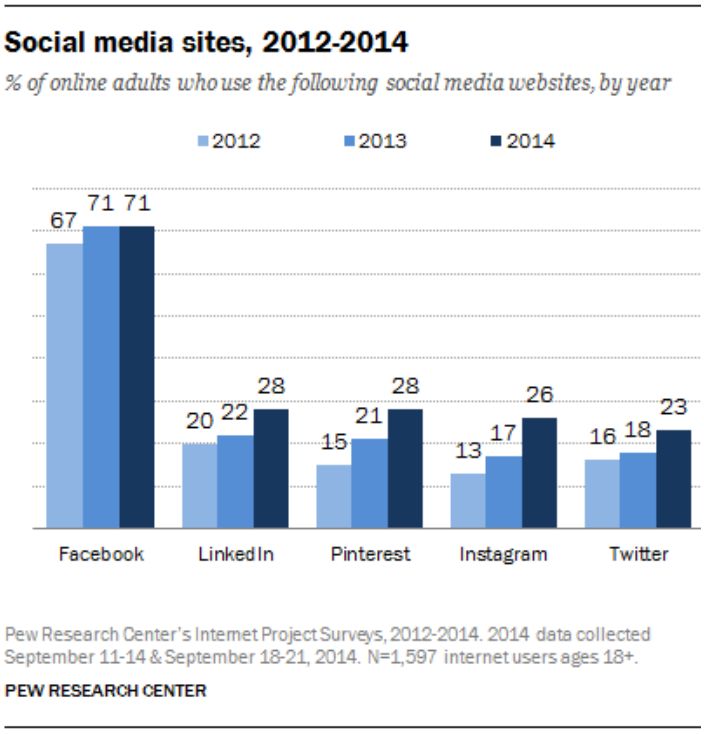


Gráfico Nº 1

El presente trabajo pretende hacer foco sobre la situación de la Red Social Facebook, precisamente por ser reconocida como aquella de mayor utilización, tanto en Argentina como a nivel mundial.

Es importante destacar la relevancia que tiene el tema para los autores, toda vez que desde la experiencia acumulada de varios años trabajando en el ámbito de la

Seguridad de la Información, se observa como con el paso del tiempo, los perfiles falsos en Facebook son una herramienta cada vez más común por parte de aquellas personas que realizan un daño. Es decir, en muchos casos los perfiles falsos de Facebook, son el medio a través del cuál se cometen delitos como injurias, extorsiones, amenazas, estafas y en los peores casos, corrupción de menores[3] y grooming.

En este sentido, la experiencia de los autores en la detección y persecución de perfiles falsos que se mal utilizan para ocasiones distintos tipos de daños, ha permitido ir delineando una serie de parámetros o patrones de comportamiento compartidos por esta clase de perfiles.

Será entonces el objeto primario de estudio del presente trabajo, la determinación, categorización y análisis de distintas clases de perfiles falsos existentes en la Red Social Facebook. Posteriormente, como objeto secundario, se analizará la relación existente entre los perfiles falsos y el mundo del cibercrimen.

Perfiles Falsos. Categorización y Finalidades:

Para el alcance de este trabajo, consideraremos que un perfil falso de Facebook es aquel que no cumple con los términos y condiciones legales establecidos por la plataforma. En la amplitud de este concepto, consideramos como perfiles falsos tanto aquellos que no pertenezcan a personas reales (nombres falsos o inventados por ejemplo, personajes de televisión, etc), aquellos que no pertenezcan a personas (por ejemplo perfiles de caricaturas, mascotas, etc), aquellos que pertenezcan a personas que tengan más de un perfil (el segundo sería considerado como en infracción puesto que sólo se permite tener un solo perfil por persona), aquellos que intenten hacerse pasar por perfiles reales existentes (alguien que se hace pasar por otra persona), entre otros casos.

También es importante hacer la precisión que podemos encontrar perfiles falsos generados de forma manual o artesanal por una persona, o bien, aquellos generados y manipualdos de forma masiva y automatizada, conocidos más comunmenten como "bots" o "robots". No obstante realizada esta aclaración, se debe considerar que en la actualidad es compleja la registración automatiza de perfiles en Facebook, toda vez que la generación automatizada es combatida por parte de los sitios y plataformas a través de distintas técnicas, entre ellas el "captcha", que básicamente se trata de pedir al usuario que ingrese una serie de letras o números que se observan en una imagen, algo bastante complicado de superar por un software automatizado.

Volviendo a los perfiles falsos, podemos adelantar que la generación de los mismos responden a distintas finalidades, entre las cuáles podemos señalar:

- **Stalker:** Perfiles utilizados para la observación y obtención de información de otros perfiles de la red social. En general este tipo de perfiles no

[3] EL LITORAL, "Condenado por corromper a menores a través de Internet", URL: http://www.ellitoral.com/index.php/diarios/2014/11/01/sucesos/SUCE-01.html, Fecha: 01/11/2014

establecen contactos o comunicaciones particulares, pero en determinadas ocasiones son generados con un objetivo ya definido, donde se puede pasar de la mera obtención pasiva de información a la obtención activa de información (contacto con engaños por ejemplo).

- **Ciberbullying:** Este tipo de perfiles se utiliza para el acoso por parte de pares, donde se busca insultar, agredir, mandar mensajes amenazantes o agraviantes desde al anonimato que permite un perfil falso.
- **Gamers:** Este tipo de perfiles se utilizan con la finalidad de obtener beneficios extras, como créditos o vidas en juegos o aplicaciones de entretenimiento.
- **Spammers:** Categoría de perfiles utilizados para la difusión masiva pero no consentida de distintos tipos de contenidos, generalmente comerciales.
- **Pornografía:** Este tipo de perfiles se utilizan para acceder, hacerse amigo de celebridades, grupos o páginas relacionadas con contenidos para adultos
- **Reputación digital:** Categoría de perfiles falsos utilizados para conseguir sumar reputación digital a través de la generación de *likes*, o bien, a través de la generación de interacción positiva falsa (como recomendación de productos).
- **Manipulación mediática:** Categoría de perfiles utilizados para la manipulación de distintos tipos de contenidos, por lo general relacionados al ámbito político o comercial. Comunmente se los puede encontrar comentando, argumentando, criticando o discutiendo en diarios digitales, o en noticias difundidas a través de la propia Red Social, con una postura muy definida con respecto a determinados temas o experiencias.
- **Cibercrimen:** Esta categoría de perfiles se utilizan como herramienta para la comisión de distintos tipos de delitos informáticos (propios o impropios), como phishing, grooming, hacking, cracking, denegación de servicios, amenazas; extorsión, difusión de malware, entre otros. En muchos casos también son utilizados para acciones previas a algunos delitos informáticos, como la realización de ingeniería social (no considerado como delito en sí). Esta categoría será analizada con mayor detalle a continuación.

Estadísticas según Facebook.

De acuerdo al informe de Facebook en Abril de 2015 ante la Securities and Exchange Commision de los Estados Unidos (SEC) -como parte de la documentación necesaria para obtener autorización para cotizar en bolsa- , se publicó que en Marzo de 2015 dicha red social cuenta con un promedio de 936 millones de Usuarios Activos Diarios (DAU – Daily Active Users), teniendo un incremento del 17% con respecto a Marzo de 2014, donde el DAU era de 802 millones.

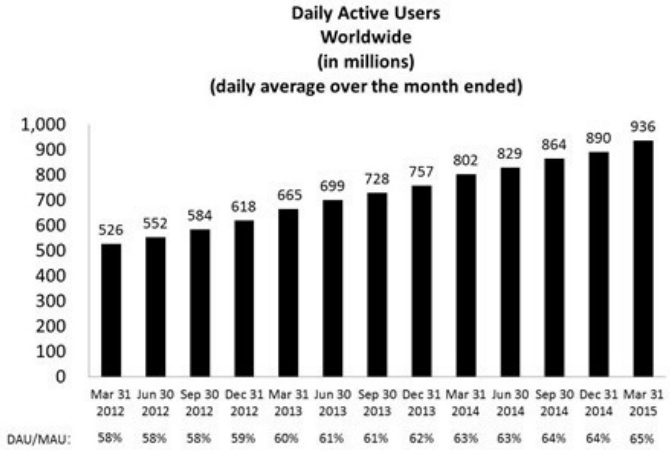


Gráfico Nº 2

Como puede observarse claramente en las estadísticas publicadas en el Gráfico Nº 1, la cantidad de usuarios sigue claramente una tendencia de crecimiento bastante regular.

Sin embargo, en este mismo informe, bajo el título de "*Limitations of key metrics and other data"* (Limitaciones en las estadísticas y otros datos), Facebook realiza una serie de consideraciones de vital importancia para el objeto del presente trabajo, toda vez que reconoce oficialmente la existencia (e incremento) de perfiles falsos en su plataforma.

En este informe Q-10 (*Quarterly Report)* de Marzo de 2012 [2], dentro del citado apartado de "*Limitations of key metrics and other data",* Facebook reconoció que:

- El 4,8% de las cuentas privadas son páginas duplicadas.
- El 2,4% del total no son cuentas humanas sino que, por ejemplo, pertenecen a mascotas o negocios con páginas que se lanzan como si se tratara del perfil de un usuario humano.
- El 1,5% de los perfiles de Facebook fue creado con intención de violar las normas de la red social, por ejemplo para el envío masivo de correos basura.
- Es decir, en la suma se reconoce que el 8,7% de los perfiles de Facebook (que equivale a alrededor de 83 millones de cuentas), es falso.

En el transcurrir de los informes cuatrimestral Q-10 de Facebook, todos ellos disponibles en el propio site oficial de "*Investor Relations*"[4] de Facebook, en Octubre de 2014, en relación a estas mismas estadísticas, podíamos observar la siguiente variación de datos:

4 FACEBOOK INC. "Investor Relations", URL: http://investor.fb.com/sec.cfm

- Entre el 4,3% y el 7,9% de los Usuarios Activos Mensuales a nivel mundial son cuentas duplicadas, en violación a sus propios términos y condiciones (aspecto que analizaremos más adelante). Llevado a los números, serían aproximadamente entre 67.65 millones y 137.76 millones de cuentas duplicadas o falsas. Nótese que la diferencia en el rango, es de aproximadamente 70 millones de cuentas.
- Entre el 0,8% y el 2,1% del total no son cuentas humanas sino que, por ejemplo, pertenecen a mascotas o negocios con páginas que se lanzan como si se tratara del perfil de un usuario humano.
- Entre el 0,4%y el 1,2% de los perfiles de Facebook fue creado con intención de violar las normas de la red social, por ejemplo para el envío masivo de correos basura.
- Es decir, en Octubre de 2014 se reconoció que en suma, entre el 5,5% y el 11,2% de los perfiles de Facebook es falso. En números, estamos hablando de entre 74.25 millones y 151.2 millones de perfiles falsos.

Para completar esta sección, construímos con una tabla de comparación sobre las estadísticas publicadas oficialmente por Facebook en relación a esta problemática, incluyendo el último informe Q-10 existente al momento de la realización de este trabajo, publicado en Abril de 2015 [3], del cuál observamos un cambio importante y sorpresivo, al menos en los términos estadísticos.

Período	Año	Cuentas duplicadas o falsas	Cuentas mal clasificadas	Cuentas indeseables
Junio	2012	4,80%	2,40%	1,50%
Septiembre	2012	4,80%	2,40%	1,50%
Marzo	2013	5,00%	1,30%	0,90%
Junio	2013	5,00%	1,30%	0,90%
Septiembre	2013	4.3% y 7.9%	0.8% y 2.1%	0.4% y 1.2%
Marzo	2014	4.3% y 7.9%	0.8% y 2.1%	0.4% y 1.2%
Junio	2014	4.3% y 7.9%	0.8% y 2.1%	0.4% y 1.2%
Septiembre	2014	4.3% y 7.9%	0.8% y 2.1%	0.4% y 1.2%
Marzo	2015	Menos de 5,00%	Menos de 2,00%	

Tabla Nº 1

Como puede observarse de la Tabla Nº 1, en un comienzo las estadísticas publicadas en cuanto a la problemática de las cuentas duplicadas o falsas tendieron hacia un crecimiento, pasando del 4,8% al 5%, y luego, a estar entre un 4,3 y 7,9% (promedio de 6,1%). Sin embargo, en Marzo de 2015, se ha optado por dejar de lado la estrategia del "rango" (que tenía la particularidad de tener un rango bastante

elevado), para volver al número directo de "menos del 5%". Cabría preguntarse: ¿Cuál es el criterio? ¿Que acciones ha realizado Facebook para volver a esta cifra de Junio de 2013?

Las novedades del 2015 no terminan allí, ya que por primera vez Facebook decide no publicar estadísticas separadas para las cuentas "mal clasificadas" y las cuentas "indeseadas". Por primera vez (y sin ninguna explicación que lo fundamente) decide que ambas puede agruparse bajo el mismo número, que ahora es de "menos del 2%".

Para cerrar esta sección, dejamos algunas características destacabables en relación al tema de estudio y su reconocimiento por parte de Facebook en los informes citados.

> "*We believe the percentage of accounts that are duplicate or false is meaningfully lower in developed markets such as the United States or United Kingdom and higher in developing markets such as India and Turkey. However, these estimates are based on an internal review of a limited sample of accounts and we apply significant judgment in making this determination, such as identifying names that appear to be fake or other behavior that appears inauthentic to the reviewers*."

De acuerdo a Facebook, ellos "creen" (creen para hacer una traducción literal) que el porcentaje de cuentas falsas o duplicadas es significativamente menor en mercados desarrollados como Estados Unidos o Reino Unido, pero significativamente mayor en mercados en desarrollo como India o Turkía.

> *"As such, our estimation of duplicate or false accounts may not accurately represent the actual number of such accounts. We are continually seeking to improve our ability to identify duplicate or false accounts and estimate the total number of such accounts, and such estimates may change due to improvements or changes in our methodology."*

Por otro lado, y como corolario de las estadísticas propias, Facebook reconoce que su estimación de cuentas falsas o duplicadas puede no ser precisa para representar el actual número de ese tipo de cuentas. No obstante y a línea posterior aseguran que están intentando mejorar su habilidad de detección de estas cuentas, buscando nuevas metodologías.

En conclusión, existe un reconocimiento por el propio Facebook acerca de su imposibilidad de determinar el verdadero número de cuentas falsas en su plataforma, por lo que a criterio de estos autores, deja abierta la pregunta sobre cuál es la metodología empleada para fundamentar las estadísticas publicadas oficialmente.

El negocio de los perfiles falsos

Como hemos podido ver anteriormente, existen diferentes categorías de perfiles falsos, generados con distintas finalidades. Algunas de ellas (gamers o stalkers) pueden ser inofensivos, pero otras tienen una clara intencionalidad de generar un daño o bien buscar un rédito económico para sí o para terceros.

En relación a este último punto tenemos que mencionar el negocio de los "*Like Farms*" o "granjas de me gusta". Básicamente, consiste en la compra de "Me gusta"

para determinadas páginas de fan, que se venden en el mercado, en sitios como "www.boostlikes.com", en donde ofrecen una determinada cantidad de likes mensuales, cada una con un costo determinado. ¿Cómo funciona o cómo es esto posible? A través de la utilización masiva de millones de perfiles falsos, que darán un "*like*" en la página de todo aquel que pague el precio.
Otro de los negocios detrás de los perfiles falsos con muchos amigos, es la propia venta de perfiles. Como se puede observar en la Imagen Nro. 3, existe un mercado de perfiles falsos con muchos amigos (cuyo valor depende de la cantidad y calidad de esos amigos), que son comprados por distintas empresas con fines publicitarios, convertidos a "Página de Fan" (borrándose en este proceso todo contenido) y listo para usarse para cualquier producto o servicio.

Imagen Nro. 3

En otro rubro distinto, pero también con finalidad económica, podemos encontrar a aquellos perfiles falsos utilizados y pagados para apoyar posturas políticas, instalar temas de agenda, desvirtuar o diluir la importancia de algunas noticias, manipular estadísticas, entre otras cosas que es posible hacer. Nuevamente, los perfiles falsos, de forma masiva, son utilizados como herramientas para lograr cualquiera de estas acciones, a cambio de un determinado precio. Es decir, existe hoy un mercado negro de manipulación digital, para cualquiera de estos fines, donde a cambio de un precio en dinero, es posible ordenar la realización de cualquiera de las acciones anteriormente descriptas.

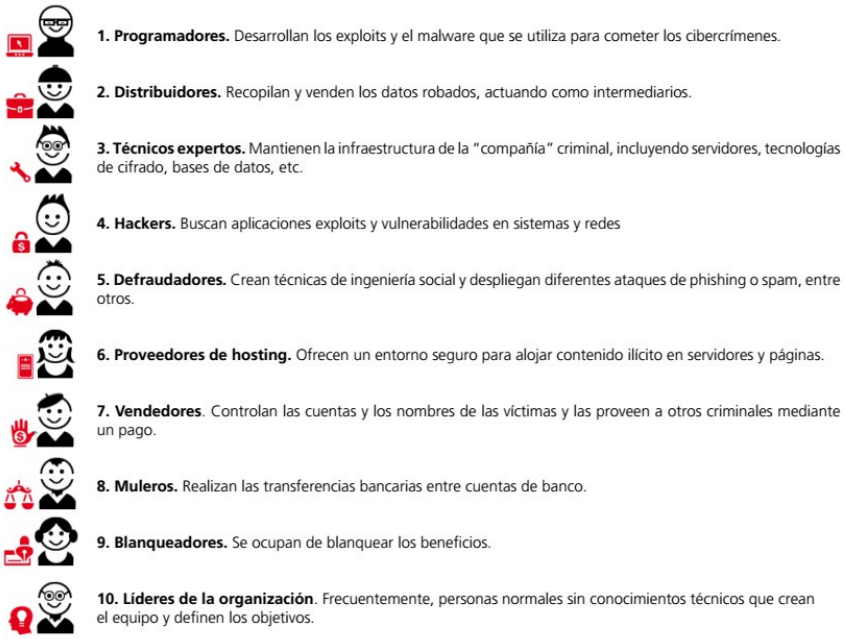
Los perfiles falsos en la cadena del Cibercrimen organizado

Según un estudio realizado por la empresa de seguridad informática McAfee [4] sobre las predicciones en materia de riesgos informáticos, el futuro esta marcado por la aparición de una nueva gama de servicios: *Hacking as a Service (HaaS)*. La proliferación de vulnerabilidades en los sistemas, combinado con un incremento de

usuarios de escasos conocimientos técnicos que se suman a la nueva generación de redes como Facebook, Twitter, Whatsapp, Line, entre otros, generan en el mercado negro de la informática un servicio destinado a satisfacer la necesidad de muchas personas que navegan la red en busca de "hackers privados" que les ofrecen la posibilidad de acceder a las cuentas de correo de sus parejas, ex-parejas, jefes, empresas, etc.

De acuerdo a otro estudio realizado por Panda Security [5], las mafias de ciberdelincuentes que operan en Internet están muy organizadas, tanto desde la óptica de visión estratégica como desde la operativa, logística y despliegue de sus operaciones. Estas mafias, no sólo pueden parecer verdaderas compañías, sino que son organizaciones multinacionales, que operan a lo largo y ancho del planeta.

De este último informe, se ha extraído una clasificación publicada por el FBI de las diferentes "profesiones" que pueden encontrarse dentro de la cadena del cibercrimen. Según el FBI, las organizaciones cibercriminales funcionan como empresas, contando con expertos especializados para cada tipo de trabajo y ocupación. Entre las especializaciones más comunes que tipifica el FBI son las siguientes:



1. Programadores. Desarrollan los exploits y el malware que se utiliza para cometer los cibercrímenes.

2. Distribuidores. Recopilan y venden los datos robados, actuando como intermediarios.

3. Técnicos expertos. Mantienen la infraestructura de la "compañía" criminal, incluyendo servidores, tecnologías de cifrado, bases de datos, etc.

4. Hackers. Buscan aplicaciones exploits y vulnerabilidades en sistemas y redes

5. Defraudadores. Crean técnicas de ingeniería social y despliegan diferentes ataques de phishing o spam, entre otros.

6. Proveedores de hosting. Ofrecen un entorno seguro para alojar contenido ilícito en servidores y páginas.

7. Vendedores. Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante un pago.

8. Muleros. Realizan las transferencias bancarias entre cuentas de banco.

9. Blanqueadores. Se ocupan de blanquear los beneficios.

10. Líderes de la organización. Frecuentemente, personas normales sin conocimientos técnicos que crean el equipo y definen los objetivos.

Las organizaciones cibercriminales se organizan de forma jerárquica, y cada paso diferente de la cadena cuenta no con uno, sino con varios especialistas. A los fines del presente trabajo, debemos prestar especial atención al eslabón número 5 del citado esquema del FBI, es decir, los defraudadores. En esta categoría encontramos aquellas personas encargadas de realizar los engaños a través de técnicas de ingenieria social

(entendida como manipulación psicológica tendiente a la obtención de información sensible), y allí es donde los perfiles falsos de Facebook son de especial utilidad.

Son estos perfiles falsos los que permiten realizar acercamientos dirigidos a la víctima, haciéndose amigos de sus amigos, estudiando sus publicaciones, entorno, horarios, gustos, etc. Una vez generada una relación de confianza con la víctima (a partir de la explotación de todos los datos publicados por la propia víctima), ya se estará en condiciones de enviar algún contenido malicioso, o bien invitarlo a acceder a algún sitio falso, entre otras posibilidades (dependiendo del tipo de ataque que se intente llevar a cabo).

Legislación aplicable y Derecho comparado

Desde una óptica netamente jurídica, surge la duda sobre si la creación y utilización de un perfil de usuario falso puede llegar a ser considerado contrario a derecho (teniendo en cuenta la legislación nacional y ya veremos la comparada). Debemos comenzar sosteniendo que en principio, la mera creación y utilización de un perfil falso no contradice ninguna normativa vigente, sino que por el contrario, podría ser considerado como una manifestación de la libertad de expresión y a modo general, representando una de las libertades más importantes que hacen que a Internet.

Sin embargo, como siempre sucede desde el Derecho, existen límites a respetar a partir de los cuáles se podría estar incurriendo en un delito penal. Uno de estos casos es donde ese perfil falso, se haga usurpando la identidad de una persona real, configurándose así un caso de usurpación o suplantación de identidad.

De acuerdo a investigaciones previas [6] en el derecho comparado se pueden encontrar diferentes tipos de estrategias legales frente a la suplantación de identidad digital. Algunos países, como EEUU y Canadá, poseen regulaciones generales para la suplantación de identidad, adaptadas de tal manera que el mismo tipo penal es aplicable tanto para el robo de identidad clásico, así como para el robo de identidad digital. A su vez, ambos completan su esquema a través de la tipificación de la tenencia ilegítima de datos de identificación personal, así como del tráfico (sin consentimiento) de estos datos. En su redacción, la Ley Federal de Canadá define la suplantación de identidad como "*la obtención y posesión de información de la identidad de una persona con la intención de engañarla o realizar actos deshonestos o fraudulentos en su nombre*". El tráfico de identidades, según este país, es un delito en el cual se "*transfiere o vende información a otra persona con conocimiento o por imprudencia y cuyo fin es la posible utilización criminal de dicha información*"[5].

EEUU, a nivel federal lo define como el que "*a sabiendas, posea, transfiera o use, sin autoridad legal, un medio de identificación de otra persona con la intención de cometer, ayudar o instigar, cualquier tipo de actividad ilegal*"[6]. Luego, algunos

5 BILL S-4, An Act to amend the Criminal Code (identity theft and related misconduct) http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=S4&Mode=1&Parl=40&Ses=2&source=library_prb

6 18 USC § 1028, "Fraud And Related Activity In Connection With Identification Documents, Authentication Features, And Information".

Estados como New York, tienen un completo desarrollo en la materia, puntualmente como derivaciones de su artículo 190[7] (*other frauds*), donde por ejemplo el Art. 190.25 (*Criminal impersonation in the second degree)*, tipifica a quien "*usurpa la identidad de otro a través de internet o medios electrónicos, con la intención de obtener un beneficio o injuriar o defraudar a otro…*". Se debe destacar que todas estas regulaciones, más allá del tipo penal objetivo -hacerse pasar por otro utilizando medios electrónicos-, incluyen un aspecto subjetivo, de manera que para que exista delito, debe también existir la intención de obtener beneficio, dañar, defraudar o injuriar. No obstante esta exhaustiva tipificación, a mediados de 2011 se presentó un proyecto[8] en el Senado de New York para agregar un tipo penal nuevo (Art. 190.87) cuya redacción es aún más precisa en el aspecto subjetivo del tipo penal. Completando la seriedad de su regulación, New York posee tipos específicos para la tenencia ilegítima de datos de identificación personal (Art. 190.81/2/3 *Unlawful possession of personal identification*), así como prevé casos especiales para exclusión del tipo (Art. 190.84, donde por ejemplo, excluye a los jóvenes menores de 21 años que se hagan pasar otros mayores para comprar alcohol).

En Argentina, no existe la figura penal para el caso anteriormente citado, sin embargo existen proyectos presentados en el Senado de la Nación Argentina que siguen la línea del derecho comparado, como el Proyecto S-1312/12 [7], donde se propone incorporar el Art. 138 bis con el siguiente texto "*Será reprimido con prisión de 6 (seis) meses a 3 (tres) años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica, a través de internet o cualquier medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para si o para terceros."*. Una variación de esta propuesta, ha sido posteriormente incorporada al Anteproyecto del Nuevo Código Penal Argentino[9], en el art. 123, inc. 3 f *"Será penado con prisión de SEIS (6) meses a DOS (2) años el que: Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio."*

Para cerrar la sección, más allá de la posibilidad de que un perfil falso pueda llegar a configurar una suplantación de identidad (y con ello un posible delito de acuerdo a la legislación aplicable), se afirma que dejando exceptuados estos casos, la creación y utilización de perfiles falsos no se encuentra regulada por la normativa vigente. Sin embargo, las diferentes acciones que pueden llegarse a realizar a través de un perfil falso (injurias, calumnias, amenazas, extorsion, corrupción de menores, y una larga lista de delitos que es posible configurar a través de las nuevas tecnologías), podrían ser consideradas como acciones típicas dependiendo de la legislación vigente en cada país [8].

---

http://www.law.cornell.edu/uscode/text/18/1028

7 Laws of New York. http://public.leginfo.state.ny.us

8 S4015A-2011: Enacts the digital impersonation prevention act. http://open.nysenate.gov/legislation/bill/S4015A-2011

9 INFOJUS, "Anteproyecto del Código Penal de la Nación", URL: http://www.infojus.gob.ar/anteproyecto-codigo-penal

Declaración de Derechos y Responsabilidades

Más allá de la situación normativa nacional e internacional aplicable a la problemática que se intenta abordar en el presente trabajo, existe otro marco normativo aplicable y es aquel dispuesto a través de la Declaración de Derechos y Responsabilidades de la propia plataforma Facebook.

Al momento de registrar una cuenta, es obligatoria y necesaria la aceptación de estos términos y condiciones legales establecidos por Facebook, entre los cuáles se pueden encontrar distintas cláusulas aplicables al tema. Entre ellas, el inciso 4to sobre "*Seguridad de la cuenta y registro*", establece que:

Los usuarios de Facebook proporcionan sus nombres e información reales y necesitamos tu colaboración para que siga siendo así. Estos son algunos de los compromisos que aceptas en relación con el registro y mantenimiento de la seguridad de tu cuenta:

1. *No proporcionarás información personal falsa en Facebook, ni crearás una cuenta para otras personas sin su autorización.*
2. *No crearás más de una cuenta personal.*
3. *Si inhabilitamos tu cuenta, no crearás otra sin nuestro permiso.*
4. *No utilizarás tu biografía personal para tu propio beneficio comercial, sino que para ello te servirás de una página de Facebook.*
5. *No utilizarás Facebook si eres menor de 13 años.*
6. *No utilizarás Facebook si has sido declarado culpable de un delito sexual.*
7. *Mantendrás la información de contacto exacta y actualizada.*
8. *No compartirás tu contraseña (o en el caso de los desarrolladores, tu clave secreta), no dejarás que otra persona acceda a tu cuenta, ni harás nada que pueda poner en peligro la seguridad de tu cuenta.*
9. *No transferirás la cuenta (incluida cualquier página o aplicación que administres) a nadie sin nuestro consentimiento previo por escrito.*
10. *Si seleccionas un nombre de usuario o identificador similar para tu cuenta o página, nos reservamos el derecho de eliminarlo o reclamarlo si lo consideramos oportuno (por ejemplo, si el propietario de una marca comercial se queja por un nombre de usuario que no esté estrechamente relacionado con el nombre real del usuario).*

A través de estos 10 incisos, Facebook establece claramente las reglas de seguridad para la creación y utilización de una cuenta. Entre las obligaciones más relevantes a los fines del presente trabajo, son los incisos 1, 2, 7 y 8.

Sin embargo, el primer inciso es el más importante para nuestro estudio, toda vez que establece al usuario de Facebook la obligación de no proporcionar información falsa, de forma que todas aquellas cuentas que entre sus datos básicos tengan algún tipo de información que no sean información real y exacta de su titular (desde una fecha de nacimiento, nombres, fotos, etc.) se encuentran en infracción, quedando disponible la posibilidad de su denuncia o reporte por no cumplir con las propias políticas aceptadas de la red social. Basados en este primer inciso, es que desde el presente trabajo se ha tomado el concepto de perfil falso anteriormente desarrollado. Entre los otros incisos de importancia encontramos la prohibición de tener más de una

cuenta personal, de forma que una segunda cuenta de la misma persona ya se encontraría en infracción.

Conclusiones

Como hemos podido observar a lo largo del trabajo, el fenómeno de los perfiles falsos en Facebook sigue en crecimiento con el paso del tiempo, siendo utilizados para una importante variedad de finalidades. Entre ellas, destacamos la utilización de los perfiles falsos de Facebook en el mundo del cibercrimen, como una herramienta de uso cotidiano por parte de los delincuentes infomáticos que utilizan a estos perfiles como medios o herramientas para llevar a cabo un importante abanico de delitos como injurias, extorsiones, amenazas, estafas y en los peores casos, corrupción de menores y grooming.

A modo de conclusión final, se destaca la necesidad de considerar el desarrollo de herramientas que permitan la detección y eliminación de los perfiles falsos, así como la adaptación o mejoramiento de políticas de acreditación de identidad ante Facebook, a fin de evitar la proliferación de esta problemática.

Referencias

[1] PEW RESEARCH CENTER, "Social Media Update 2014", Url: http://www.pewinternet.org/2015/01/09/social-media-update-2014/, Consulta: 20/04/2015

[2] MCAFEE LABS, "Threats Predictions", 2013. Url: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf, Consultado: 27 de Noviembre de 2013

[3] PANDA SECURITY, "El mercado negro del Cibercrimen", 2010. Url: http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf, Consultado: 27 de Noviembre de 2013

[4] UNITED STATES SECURITIES AND EXCHANGE COMMISSION, FORM 10-Q - For the quarterly period ended June 30, 2012 - Url: http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm – Consulta: 23/04/2015

[5] UNITED STATES SECURITIES AND EXCHANGE COMMISSION, FORM 10-Q - For the quarterly period ended March 31, 2015 – Url: http://investor.fb.com/secfiling.cfm?filingID=1326801-15-15&CIK=1326801 – Consulta: 23/04/2015

[6] TEMPERINI, Marcelo y BORGHELLO, Cristian, "Suplantación de Identidad Digital como delito informático en Argentina", Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 41 - 2012. ISSN 1850-2814

[7] Honorable Congreso de la Nación. Ingresado en fecha 15/05/2012, Expediente Nro. 1312/12 – URL: http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1 [15/06/2012]

[8] TEMPERINI, Marcelo, "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 2dra. Parte."; Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 43 - 2014. ISSN 1850-2814