Suplantación de Identidad Digital como delito informático en Argentina.

Lic. Cristian Borghello[1]; Abog. Marcelo G. I. Temperini[2]

Abstract Español. La identidad digital, entendida como el conjunto de rasgos y características particulares que una persona expresa a través de internet, forma una parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral. Esta identidad digital se encuentra en situación de crisis, debido a los constantes y crecientes embates por parte de ciberdelincuentes en todo el mundo. Dentro de este marco, el objetivo del presente trabajo será establecer las raíces de esta creciente actividad delictiva, analizando los diferentes modos de ejecución, su impacto y consecuencia en las víctimas, así como la legislación existente en la materia. Finalmente se concluye con una propuesta de tipificación penal del delito suplantación de identidad digital, así como de la tenencia y transferencia ilegítima de datos de identificación personal.

Abstract en Inglés: The digital identity, understood as the gathering of features and particular characteristics that a person expresses through the internet, is an indivisible part of the personal identity of every subject, in his dynamic face, and more precisely in his psychological, social and moral aspect. This digital identity founds itself in a situation of crisis, due to the constant and growing attacks by cybercriminals all over the world. Within this context, the goal of the present work will be to stablish the roots of this growing criminal activity, analizing the different ways of execution, its impact and consecuences on the victims, as well as the existing legislation in this area. Finally it will be concluded with a proposal of penal typification of the crime of digital identity subrogation, as well as the possession and transference of data of personal identity.

Keywords: delitos informáticos, suplantación de identidad, robo de identidad, privacidad, penal

[1] Licencido (UTN) en Sistemas y certificado internacional en seguridad de la información. Creador y Director de los sitios Segu-Info –www.segu-info.com.ar– y Segu-Kids –www.segu-kids.org– especializados en Seguridad de la Información Seguridad para la familia. Contacto: info@segu-info.com.ar

[2] Abogado (UNL) especializado en Derecho Informático. Director de la Red Iberoamericana de Derecho Informático – elderechoinformatico.com. Analista de Seguridad y Director de AsegurarTe – Consultora en Seguridad de la Información. Contacto: temperinimarcelo@gmail.com

"Puedo dividir mi mente. Cada vez se me da mejor. Puedo verme a mí mismo como dos, tres o más personas. Cuando voy de ventana en ventana, activo primero una parte de mi mente y, luego otra. La vida real no es más que otra ventana, y no necesariamente la mejor que tengo".

Un usuario de Internet.

Introducción

Cuando el hombre iba de a pie y descalzo sobre las llanuras de la tierra, su sola presencia física era suficiente para demostrar su identidad. Con el pasar de los siglos y con la necesidad, pero imposibilidad de estar en dos lugares a la vez, se debieron crear métodos eficientes para comunicarse y demostrar quién enviaba un mensaje determinado. En la era de la información, con miles de maneras de comunicarse a disposición del ser humano, la necesidad de identificarse y de proteger dicha identidad para que no sea utilizada por terceros, se ha vuelto imprescindible al punto tal que la "identidad", eso que vuelve "individuo único" a una persona, será la moneda de cambio de las futuras generaciones, incluso para aquellas que prefieren ser anónimos (*anonymous*) o utilizar pseudonimos (*nicknames*) en internet.

Identidad e identidad digital

Sin profundizar en este momento en conceptos jurídicos, la **identidad** se puede definir como el carácter distintivo, aquel conjunto de atributos y características que permiten individualizar a la persona en sociedad, pertenecientes a un individuo determinado, o compartidas por todos los miembros de una determinada categoría o grupo social. Según Rummens, el término proviene de la palabra francesa "*identité*" que tiene sus raíces lingüísticas en el sustantivo latino "*identitas*", una derivación de "*idem*", que significa "lo mismo".

Por consiguiente, el concepto acuñado como **identidad digital** representa esas mismas características y actividades pero llevadas a cabo en internet, como consecuencia del crecimiento de las comunicaciones digitales. Esta identidad es a la que generalmente se refiere como "vida virtual".

Crecimiento de actividades delictivas relacionadas con la identidad

Si bien es difícil obtener estadísticas que demuestren en forma efectiva y precisa el crecimiento de las actividades delictivas relacionadas al robo de identidad, diversos estudios internacionales demuestran que el **robo de identidad digital** se ha transformado en el delito del milenio y es una de las actividades ilícitas de mayor crecimiento de la última década.

En febrero de 2012, la Federal Trade Commission (FTC) publicó su lista sobre las quejas más comunes de los consumidores de EE.UU.[3] y, por cuarto año consecutivo, el robo de identidad encabezó la lista: de 1,8 millones de denuncias presentadas en 2011, el 15% fueron sobre de robo de identidad y cerca del 25% estaban relacionadas con el fraude fiscal o los salarios. Por su parte, el Internal Revenue Service (IRS) dijo que *"el robo de identidad es una de las formas más comunes de estafas y se están encontrando cada vez más delincuentes en busca de nuevas maneras para utilizar la identidad y la información personal del contribuyente"* [4].

América Latina no es ajena a estas estadísticas y la carencia de números oficiales no es excusa para evitar el problema e ignorar a la gran cantidad de personas que cada día ven afectados su honor, su reputación, su trabajo, su imagen, su salud social y psicológica y sus actividades financieras y económicas, debido a que terceros han usurpado su identidad.

Durante 2010, las autoridades financieras de México recibieron 880 denuncias diarias por robo de identidad y reportaron pérdidas anuales por aproximadamente 9 millones de dólares. Ello originó que el pasado Diciembre de 2011 México reformara su Código Penal Federal, para tipificar el robo de identidad dentro de las figuras de fraude específico y penalizar hasta con 12 años de prisión a quien utilice indebidamente cualquier tipo de identificación de otra persona[5].

Un informe sobre cibercrimen del Reino Unido basa el cálculo de las pérdidas por robo de identidad digital según la cantidad de usuarios con acceso a internet y la probabilidad de que cada uno de ellos sea afectado por este tipo de delito[6]. Tomando como referencia esta metodología, a continuación se realiza una estimación del monto de pérdidas por robo de identidad en América Latina:

- De acuerdo a lo informado por Internet World Stats, hasta junio de 2011 había 212 millones de personas conectadas en América[7].
- El estudio del Reino Unido estima que el 25% de los robos de identidad se realiza en línea a través de Internet -robo de identidad digital-.
- Según la Federal Trade Commission, 9 millones de personas son afectadas por este delito cada año en EEUU[8] y, si se considera su población de 310 millones de habitantes, se puede deducir que el 2,9% de ellos sufriría un robo

[3] Federal Trade Commision (FTC). "Consumer Sentinel Network Data Book". Febrero 2012. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf [28/02/2012]

[4] Internal Revenue Service (IRS). "Dirty dozen tax scam of 2012". Febrero 2012. http://www.irs.gov/newsroom/article/0,,id=254501,00.html [28/02/2012]

[5] Boletín Nro 4.520. Cámara de Diputados de México. "El robo de identidad origina en México pérdidas anuales por 9 millones de dólares". Publicado el 18 de diciembre de 2011. http://www3.diputados.gob.mx/camara/005_comunicacion/a_boletines/2011_2011/012_diciembre/18_18/4520_el_robo_de_identidad_origina_en_mexico_perdidas_anuales_por_9_millones_de_dolares_favor_de_utilizar_de_domingo_para_lunes [18/02/2012]

[6] Detica - Cabine Officce. "The Cost Of Cyber Crime". Noviembre de 2011. Pág. 18. http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime [18/02/2012]

[7] Latin American Internet Usage Statistics. "Internet Users, 20-Jun-11". http://www.internetworldstats.com/stats10.htm [18/02/2012]

[8] Federal Trade Commission (FTC). "About Identity theft". http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html [18/02/2012]

de identidad. Estos datos coinciden con los publicados por Bureau of Justice Statistics que, en Noviembre de 2011, publicó que 8,6 millones de miembros de la comunidad norteamericana había experimentado uno o más tipos de victimización relacionados con la identidad[9].

- En 2006, la Consultora Gartner estimó que el costo del robo de identidad es de al menos 572 dolares por víctima, ya que esta recupera sólo el 54% de las pérdidas totales que ascienden a promedio a un valor de 1.244 dólares.

Si se proyectan estos valores, se puede calcular el monto de pérdidas anuales para América Latina: 212 millones de habitantes x 2,90% de afectados x U$S 572 de pérdidas individuales = 3.250 millones de dólares en pérdidas por robo de identidad y 880 millones de dólares (25%) en pérdidas por robo de identidad digital. De acuerdo a un estudio de ComScore, el número de usuario de conectados en América Latina creció al menos 15% en el último año, lo que también brinda una idea bastante precisa de lo que podrían llegar a crecer las actividades delictivas relacionadas.

Con respecto a estos montos deben hacerse consideraciones adicionales: (i) el monto de 572 dólares es un promedio y puede estar por debajo del costo real que pierde un damnificado; (ii) muchas personas no denuncian el robo de identidad porque actualmente no representa un delito en la mayoría de los países o simplemente no saben que pueden hacerlo; muchas entidades bancarias prefieren no denunciar debido a la pérdida de imagen en seguridad que ello significaría (iii) otros estudios demuestran que del 38% al 48% de los damnificados se entera de las acciones contra su identidad, luego de los tres primeros meses y que del 9% al 18% se entera luego de pasados al menos 4 años[10], siendo muy difícil de calcular todos los tipos de daños y costos en los que se incurren durante este período.

Actividades y consecuencias relacionadas al robo de identidad

El robo de identidad puede ocurrir de diversas maneras aunque los elementos básicos y la finalidad son los mismos: la obtención de información personal para realizar algún tipo de perjuicio. Para analizar estas actividades es importante destacar la diferencia entre el robo de identidad y la **impersonalización**, que sucede simplemente cuando alguien se hace pasar por otra persona u organización. Si bien en la mayoría de los casos el robo de identidad se basa en la impersonalización para efectuar una acción delictiva, puede suceder que la impersonalización sólo se realice con "fines más inocentes" como puede ser el hacerse pasar por un famoso, hablar en nombre de otro o intentar obtener descuentos utilizando su identidad. Leyes locales en New York, EEUU[11], consideran este tipo de diferencias al momento de imponer castigos a los responsables.

[9] LANGTON Lynn, Bureau of Justice Statistics, NCJ 236245, "Identity Theft Reported By Households, 2005-2010". 30 de noviembre de 2011.
http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2207 [18/02/2012]
[10] Spend on Life. "Official Identity Theft Statistics". Año 2009.
http://www.spendonlife.com/guide/identity-theft-statistics [18/02/2012]
[11] New York Stae Law. Penal Laws. Article 190, "Other frauds".
http://ypdcrime.com/penal.law/article190.htm [15/02/2012]

Como se ha visto anteriormente, el problema no es fácil de dimensionar y algunas de las consecuencias para las víctimas tampoco lo son. En general, se puede categorizar a cuatro tipos de víctimas: los gobiernos, las empresas privadas que manipulan gran cantidad de datos personales, los servicios financieros y, principalmente, a los clientes y usuarios.

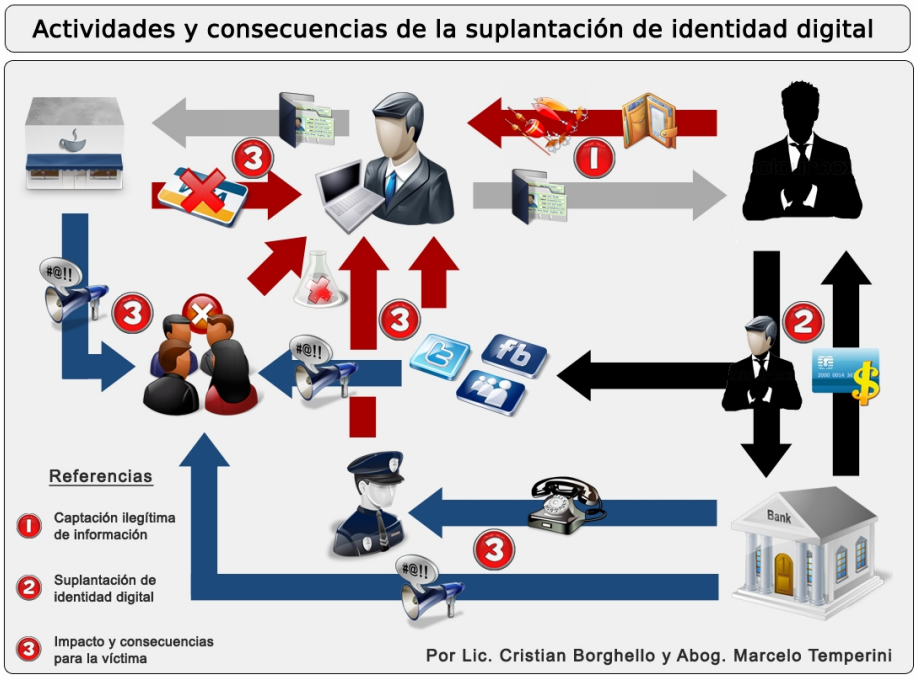

Imagen 1 – Actividades y consecuencias de la suplantación de identidad digital

Recolección de información

La recolección de información personal y sensible puede ser física o virtual, y algunas de las técnicas que existen para apoderarse de esta información son:

- Robo de documentación personal, arrebatos de billeteras, carteras, bolsos, etc.
- *Dumpster diving* (hurgar en la basura)*:* recolección de documentación que fue descartada o arrojada a la basura.
- Robo de información a través de empleados deshonestos en organizaciones que manipulan los datos personales.
- *Skimming*: obtención de información de las bandas magnéticas de tarjetas de crédito o débito con la finalidad de reproducir o clonar dicha tarjeta y luego utilizarla con fines delictivos.
- Phishing y *scam* (estafa): recolección de información personal a través de diversos métodos tecnológicos en los cuales se busca engañar a la víctima

para que revele esa información. El método más común -pero no el único- es el envío de correos electrónicos o SMS utilizando la imagen de una empresa u organización conocida y buscando que la víctima ingrese su información personal en un sitio web exactamente igual al original pero administrado por el delincuente.

Esta actividad también se puede realizar a través del teléfono, fax o cualquier otro medio, ya que la masificación de las comunicaciones digitales ha facilitado la obtención de información personal. Si bien las técnicas pueden variar en el tiempo, ser más simples o más complejas, siempre tienen un fuerte componente de **ingeniería social**, en el cual se engaña y manipula psicológicamente a la víctima para que revele datos personales que no brindaría en circunstancias normales.

Tipo de información recolectada

La información que los delincuentes buscan obtener está siempre íntimamente relacionada con el perfil personal, social, psicológico, sociológico, espiritual, intelectual, financiero, económico, físico, virtual de un individuo, vivo, muerto, existente en la realidad o no. Algunos de los datos recolectados corresponden a:

- Documentación personal -documentos de identificación, pasaportes, tarjetas, etc- ya sea de forma física o digitalizada.
- Perfil virtual de la víctima, relacionado a la información que se puede encontrar de la misma en su correo electrónico, foros, redes sociales, buscadores o simplemente por su interacción social en la red.
- Información financiera: números de cuenta, PIN, tarjetas de crédito y débito o cualquier dato que brinde al delincuente la posibilidad de cometer acciones fraudulentas.

Cabe señalar que uno de los principales aspectos que colabora para que ésta actividad siga creciendo es que la sociedad carece de la capacitación y concientización necesaria para proteger su documentación y su identidad, y que desconozca el potencial peligro de la información asociada a su persona en las manos inadecuadas.

Finalidad e impacto del robo de identidad

Más allá de las pérdidas financieras y económicas directas ya señaladas, también existen otros tipos de daños que pueden ser causados a las víctimas de una suplantación de identidad digital. Entre esas posibilidades, se encuentra la injuria a través de las redes, provocando un serio daño al buen nombre, la honra y la reputación de la víctima. Como se verá detalle más adelante, el principal inconveniente para la persona afectada está asociado al impacto social, psicológico y moral que implica que su identidad puede ser utilizada por un tercero. Dicho efecto es producido como consecuencia de que el delincuente, al suplantar la identidad digital del afectado (robando sus nombres de usuarios, ID y contraseñas en el correo electrónico, redes sociales, foros y en cualquier otra plataforma que la víctima utilice), ocasiona que la misma pierda parte de su vida, aquella que desarrolla.

Con respecto a las principales finalidades por las cuáles un delincuente está interesado en hacerse pasar por otra persona, podemos encontrar:

- Efectuar gastos con tarjetas, solicitar cambios de domicilio, abrir nuevas cuentas, obtener créditos, emitir cheques sin fondos, falsificar documentación, obtener documentos de identidad, obtener un empleo, presentar declaraciones de impuestos fraudulentas, etc.
- Adquirir productos y/o contratar servicios usando el nombre de la víctima y contrayendo deudas en su nombre.
- Crear perfiles falsos en distintas redes y comunidades en internet, con finalidad de afectar la reputación, la honra y el buen nombre de la víctima, o bien, afectar la de terceros.
- Hacerse pasar por la víctima con la finalidad de adquirir información confidencial y secreta, que sólo debería ser accesible por su titular (por ejemplo, una vez que ha accedido a un sistema de mensajería electrónica con la cuenta de la víctima, se contacta con terceros solicitando información confidencial).

Diferenciando responsabilidades

En relación a los diferentes sujetos que llevan adelante actividades delictivas relacionadas al robo de identidad digital, se pueden identificar dos grandes grupos:

- Aquellos delincuentes que actúan solos, generalmente de una franja etaria de menores de 25 años y con conocimientos técnicos limitados pero que sirven a sus objetivos. En América Latina la mayoría de los delitos relacionados al phishing son cometidos por este tipo de personas.
- Grupos delictivos organizados, compuestos por personas con distintas especialidades y recompensas de acuerdo a sus funciones del riesgo que asumen dentro del grupo. En este caso se destacan grupos de Europa del Este, EEUU y Brasil.

Si bien no puede existir el delito como tal sin la participación de los grupos anteriores, según lo ya señalado sobre la falta de educación del usuario, también cabe cierta responsabilidad al mismo, dado que por lo general no se suele proteger de manera adecuada la información personal, entregándola ante el más mínimo engaño o ante la ingenuidad de obtener un supuesto “beneficio” por ello. Ejemplos de este tipo de comportamiento son las loterías falsas que prometen premios millonarios con sólo enviar un nombre y apellido, o las cadenas de correo electrónico que ofrecen ventajas adicionales a quienes realicen tal o cual acción, a cambio de entregar información personal.

Otro responsable en la cadena son las entidades comerciales, financieras y crediticias que conceden servicios, créditos y entrega de fondos a terceros no apropiadamente identificados, o que realizan controles débiles y fácilmente evitables por los delincuentes. En Argentina, la Ley Nº 25.246, establece la obligación para las

financieras (junto a otros tantos sujetos obligados) a recabar de los usuarios los documentos que prueben fehacientemente su identidad[12].

Según el Dr. Gabriel Martinez Medrano, "*desde el punto de vista civil, la víctima está en condiciones de reclamar a la entidad una indemnizacion por daños si esta otorgó un crédito a un tercero y ese otorgamiento le causó un perjuicio... La impotencia [de la víctima] frente al error genera necesariamente mayores angustias por cuanto da cuenta de una situación injusta, máxime cuando se mantuvo durante un largo tiempo... Los tribunales han reiterado en numerosas oportunidades que la apertura de crédito sin contar con los recaudos legales necesarios genera responsabilidad bancaria*".

Finalmente, la negligencia del Estado también lo transforma en parte responsable, porque posibilita la comisión del delito a través de la falta de normativa, campañas de concientización y controles indispensables a la documentación del ciudadano, la dificultad para denunciar el delito y sobre todo la ausencia de auditorias -que existen en la teoría pero son ineficientes en la práctica- impuestas a empresas de servicios y entidades financieras y crediticias mencionadas anteriormente.

Independientemente de la forma en que sea realizada la obtención de información, uno de los puntos más importantes a tener en cuenta es que la acción delictiva puede ser llevada en varios países -delitos sin fronteras o transnacionales-, lo que hace necesario el tratamiento de tratados o convenios internacionales que regulen y castiguen estas actividades.

La identidad digital como bien jurídico protegido

Para dar inicio a esta sección, se debe analizar el concepto y protección tradicional de la identidad de las personas, tanto físicas como jurídicas, las cuales no han sido excepción a la serie de cambios y mutaciones que han producido las nuevas tecnologías sobre una gran cantidad de institutos.

Entre los conceptos clásicos, se puede citar un importante fallo italiano, en el cuál se expresó que la identidad era "el conjunto de atributos, calidades, caracteres y acciones que distinguen a un individuo con respecto a cualquier otro, y que conforma su derecho a ser reconocido en su 'peculiar realidad'[13]. A través de su famoso libro "Derecho a la Identidad", el jurista peruano Fernando Sessarego, supo dotar de mayor precisión al concepto buscado, afirmando que se trataba de un conjunto de atributos y características que permiten individualizar a la persona en sociedad, donde ese plexo de características de la personalidad de cada cual se proyecta hacia el mundo exterior

12 Ley Nº 25.246. Art. 21. "Las personas señaladas en el artículo precedente quedarán sometidas a las siguientes obligaciones: a. Recabar de sus clientes, requirentes o aportantes, documentos que prueben fehacientemente su identidad, personería jurídica, domicilio y demás datos que en cada caso se estipule..."
http://infoleg.gov.ar/infolegInternet/anexos/60000-64999/62977/texact.htm [20/02/2012]

13 Corte Suprema italiana, 13 VII 71, Foro Italiano, 1972 I 432

y permite a los demás conocer a la persona, a "cierta persona", en su "mismidad", en lo que ella es en cuanto particular y específico ser humano[14].

Como se puede observar, se trata de un concepto que no se limita a considerar el aspecto fisico o biológico de la persona; comprende también el aspecto espiritual, intelectual, religioso, social, profesional y psicológico, a través del cual el individuo se proyecta socialmente al exteriorizar por algún medio esos aspectos propios de su personalidad. Por eso la doctrina ha señalado desde hace tiempo que puede hablarse de una doble faz en la identidad personal: la estática, que apunta a los rasgos fisicos y biológicos del individuo, inmutables por naturaleza; y la dinámica que se refiere a los modos particulares que ese sujeto adopta para comunicarse e insertarse en su vida de relación con los demás[15].

Un instrumento jurídico cercano a la protección jurídica de la identidad personal es la Convención Americana de Derechos Humanos, en la cuál se expresa que "toda persona tiene derecho a que se respete su integridad fisica, psíquica y moral"[16]. En su Art. 11[17] se hace especial detalle sobre la protección de la honra y la dignidad de las personas, elemento que es de suma utilidad al momento de analizar los efectos dañinos de la suplantación de identidad y la justificación en su protección. A su vez, otro elemento de protección de los derechos humanos más reciente, tal como la Declaración Universal sobre Bioética y Derechos Humanos[18], reconoce entre sus considerandos que la "identidad de una persona comprende dimensiones biológicas, psicológicas, sociales, culturales y espirituales".

Desde el punto de vista penal argentino, la identidad personal es considerada como un bien jurídico a proteger dentro del Título IV (Delitos contra el Estado Civil) Capítulo II (Supresión y suposición del estado civil y de la Identidad), aunque también se pueden encontrar otras formas de protección a la identidad, así como el Art. 292 del Código Penal, ubicado dentro del Título XII (Delitos contra la fe pública), Capítulo III (Falsificación de documentos en general), donde se sanciona al "*que hiciere en todo o en parte un documento falso o adultere uno verdadero, de modo que pueda resultar perjuicio...*". Este último delito citado, es de vital importancia dado que en general, el delito de suplantación de identidad digital tiene una estrecha vinculación en cuanto operatoria y finalidad.

---

[14] FERNÁNDEZ SESSAREGO, Carlos, "Derecho a la Identidad Personal", Astrea, 1992, pág. 55.

[15] CABRERA, Delma Y CODEGLIA, Luis María, "Responsabilidad por violación al derecho a la identidad". Publicado en "La responsabilidad (Homenaje al profesor Doctor Isidoro H. Goldenberg)". 1ra. edición, 1995

[16] Convención Americana de Derechos Humanos (CADH). Pacto de San José de Costa Rica. 1969

[17] CADH. Art. 11. Protección de la Honra y de la Dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

[18] UNESCO. Declaración universal sobre Bioética y Derechos Humanos. 19 de octubre de 2005.
http://unesdoc.unesco.org/images/0014/001428/142825s.pdf#page=85 [18/02/2012]

Al analizar los conceptos citados a la luz del título de esta sección, se puede adelantar que la identidad digital debe ser un bien jurídico protegido. Es decir, teniendo en consideración la amplitud de los conceptos de identidad mencionados, se puede afirmar que la identidad digital que una persona desarrolla a través de internet forma también parte de ese todo único e inseparable que es su identidad personal. Su ubicación podría depender de las interpretaciones pero, a entender del presente, forma parte de una faceta social y psicológica de la persona, o más genéricamente se la podría ubicar dentro de la faz dinámica de la identidad. No obstante, dicha postura se explicará con mejor detalle en la próxima sección.

Importancia de la identidad digital en la era de internet.

Como ha sucedido a través de los años, las nuevas invenciones del hombre han ido modificando, en mayor o menor medida, tanto su manera de realizar actividades como la de relacionarse con otras personas. Internet ha marcado un antes y un después, evolucionando la manera de trabajar, de compartir, de adquirir conocimiento, de divertirse, de establecer relaciones con otras personas y grupos de interés, incluso, en la manera de cometer ilícitos. Las relaciones en la vida moderna suelen tener un alto componente tecnológico y son ejemplo de ello nativos digitales que se ha enamorado a través de un chat, han tenido sus peleas de pareja a través de la red, e incluso algunos algunos han terminado relaciones a través de un SMS.

Según estudios de telecomunicaciones[19], en 2010 en Argentina existieron 53 millones de suscripciones de telefonía celular, es decir, que la tasa de celulares es de aproximadamente 13 celulares por cada 10 personas. Esta tendencia hacia la hiperconectividad tiene sus consecuencias en los individuos, sus comportamientos y "necesidades". Un reciente estudio realizado por el psicólogo Wilhelm Hofmann de la Universidad de Chicago, Illinois (EEUU), publicado en la revista especializada *Journal of Psychological Science*, demostró que el uso de las redes sociales ya aparece entre el ranking de las adicciones. Entre las actividades más adictivas en internet, *"twittear"* ha quedado en el escalón más alto, seguido por el muro de Facebook o las novedades en los círculos de Google+. En una entrevista con el diario The Guardian del Reino Unido, Hofmann afirmó que el deseo por las redes sociales "puede ser comparativamente más difícil de resistir" que el evocado por el tabaco o el sexo, "debido a su alta disponibilidad y porque se sienten como si no costara demasiado participar", socializarse con ellas. A esto se une un "coste monetario" percibido como prácticamente nulo por las personas.

Estas consecuencias son fáciles de observar en cualquier colegio primario o secundario, donde los celulares, reproductores portátiles y demás dispositivos electrónicos, suelen traer importantes problemas a directivos y docentes desde hace ya varios años. Son los adolescentes la franja etárea quizás más "afectada" por las nuevas tecnologías, dado que su condición de nativos digitales -aquellos que nacieron con la tecnología en sus manos- le hace muy complicado concebir sus vidas sin algún

[19] ITU World Telecommunication / Mobile cellular subscriptions statistics. http://www.itu.int/ITU-D/ict/statistics/material/excel/2010/MobileCellularSubscriptions_00-10.xls [18/02/2012]

tipo de conexión y "*updates*" constantes en las redes. Así lo demuestra otro estudio realizado entre jóvenes[20], donde se dejó a 200 estudiantes sin conexión a ningún tipo de tecnología, que según los psicólogos mostró síntomas se corresponden a aquellos que sufren las personas que acaban de abandonar una adición, como las drogas o el alcohol: ansiedad, sensación de miseria, cambios emocionales y sensación de soledad fueron algunos de los síntomas, según señalaron los responsables del informe. ¿Cuál es el motivo? Un estudiante señalaba que para él, poder enviar mensajes a sus amigos le proporcionaba una "sensación de confort" que había perdido durante el aislamiento. "Me sentí como una persona en una isla desierta" dijo el jóven.

En su estudio "Identidad en Internet", Sherry Turkle[21] mostró las consecuencias psicológicas de que una persona pueda, a través de las nuevas tecnologías, mostrarse como alguien más, expresando así diferentes identidades. Uno de los sujetos en estudio, expresó que, gracias a internet: *"Puedo dividir mi mente. Cada vez se me da mejor. Puedo verme a mí mismo como dos, tres o más personas. Cuando voy de ventana en ventana, activo primero una parte de mi mente y, luego otra. La vida real no es más que otra ventana, y no necesariamente la mejor que tengo"*.

Más allá de la existencia de casos extremos de adicción a las tecnologías, lo cierto es que en la actualidad, la mayoría de las personas con acceso a las redes experimentan la necesidad de "estar conectados", de chequear sus casillas de correo electrónico, su timeline de twitter o su muro en facebook. Es en esta participación virtual y social donde las personas expresan sus deseos, sus intereses, sus amistades, su trabajo, sus proyectos, en suma, una parte importante de sus vidas. Este es el punto donde se encuentra la identidad digital de las personas, en movimiento constante y dinámico, ese mencionado conjunto de atributos y características que permiten individualizar a la persona en un grupo social, atributos y características que cada vez más se desarrollan en y a través de internet.

¿Donde se pueden encontrar esos rastros? Depende de la persona, si fuera un joven probablemente sería su perfil de Facebook, su *Timeline* de Twitter, o hasta hace algún tiempo, hubiese sido su Fotolog. Cualquier actividad de la red es apta para ir trazando una identidad, desde la participación en foros, blogs, comunidades de interés, o en las propias redes sociales. Es, en definitiva, el espacio donde el sujeto se siente más a gusto para expresar lo que siente, lo que quiere, lo que le molesta, lo que lo hace ser él y no otra persona, pero en la red. Así va forjando su identidad digital a medida que pasa el tiempo, identidad que es reconocida -y juzgada- por otros sujetos en la red. Actividades que pueden ser aprobadas con un contador de pulgares arriba; con más puntos (que le permitan ser un usuario de mayor nivel, diferenciandose del resto) o muchos comentarios, según el tipo de plataforma que utilice. También pueden realizarse acciones rechazadas por sus pares, ya sea con comentarios negativos o incluso con el apartamiento de la propia comunidad, ya que cada grupo posee sus propios códigos de comportamiento o meritocracia, por ejemplo, al momento de compartir contenidos (donde en caso de ser inadecuados, pueden ser descartados por

[20] A Day without Media. Research conducted by ICMPA and students at the Phillip Merrill College of Journalism, University of Maryland, College Park, USA. http://withoutmedia.wordpress.com/ [19/02/2012]

[21] Profesora de Sociología de las ciencias en el Massachusetts Institute of Technology, miembro de la Sociedad Psicoanalítica de Boston, autora de varios libros sobre el tema y psicóloga clínica en ejercicio

los propios usuarios), haciendo que la acción colectiva decida que se queda y que se va, en un claro ejercicio de autogestión o autocontrol de la red.

Legislación comparada

En el derecho comparado se pueden encontrar diferentes tipos de estrategias legales frente al robo de identidad digital. Algunos países, como EEUU y Canadá, poseen regulaciones generales para el robo 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 el robo 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*"[22].

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*"[23]. Luego, algunos Estados como New York, tienen un completo desarrollo en la materia, puntualmente como derivaciones de su artículo 190[24] (*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[25] 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).

[22] 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 [18/02/2012]

[23] 18 USC § 1028, "Fraud And Related Activity In Connection With Identification Documents, Authentication Features, And Information". http://www.law.cornell.edu/uscode/text/18/1028 [18/02/2012]

[24] Laws of New York. http://public.leginfo.state.ny.us [20/02/2012]

[25] S4015A-2011: Enacts the digital impersonation prevention act. http://open.nysenate.gov/legislation/bill/S4015A-2011 [19/02/2012]

A su vez, en plena conciencia que una **adecuada tipificación no es suficiente**, EEUU y Canadá han formado un proyecto en conjunto, bajo el nombre clave de IC3 (*Internet Crime Compliance Center*), a través del cual las víctimas de delitos en línea, incluyendo el robo de identidad, puede informar de una posible actividad criminal. El personal de IC3 analiza estas quejas en patrones y niveles de posible conducta delictiva y, en su caso, ofrece información para la investigación de la denuncia, así como otro tipo de información a los fiscales o autoridades federales, estatales o locales. Son este tipo de organizaciones, los aspectos claves para el éxito en el combate contra el cibercrimen, ya que a diferencia de lo que se informa por los medios masivos de comunicación, y lo que la sociedad cree entender, la sola tipificación legal no opera como solución mágica sobre los delitos. Se debe contar con un centro especializado, con personal capacitado, que sepa ser un nexo entre las víctimas de delitos informáticos y el Estado, encargado de la persecución de estos hechos.

En el Reino Unido, el robo de identidad es "*el acto por el cual alguien obtiene información suficiente acerca de la identidad de otro para facilitar el fraude de identidad, con independencia de que la víctima esté viva o muerta*"[26]. Más allá del tipo básico, esta tipificación tiene el agregado de mencionar la independencia sobre la vida de la víctima, a lo cuál, surge la pregunta ¿Se puede suplantar la identidad de una persona muerta? La respuesta es positiva, ya es posible que un delincuente se haga pasar por alguien que ha fallecido, aprovechando de que terceros aún no han tomado noticia del deceso, y obteniendo así beneficios que no les pertenecen. Por ello, parece acertada su incorporación al tipo penal, a fin de precisar el abanico de casos que quedarían comprendidos en su redacción.

Prevención y mitigación de los efectos del robo de identidad

No existe un procedimiento infalible que pueda ser utilizado para evitar y prevenir el robo de identidad ya que, como se analizó, esta actividad puede ser llevada adelante de diversas maneras y cada persona puede ser afectada por varias de ellas. A continuación se detallan algunos puntos a considerar para prevenir el robo de identidad y también algunos consejos útiles en caso de sospechar que ya se fue víctima de esta actividad.

Inicialmente es efectivo tomar medidas de prevención y, en caso de perder documentos o información digital que contengan datos personales, puede ser útil reaccionar rápidamente tomando determinadas medidas y así minimizar la posibilidad de convertirse en víctima del robo de identidad:

- Cerrar inmediatamente cualquier cuenta relacionada a la información perdida o, en su defecto informar a la entidad afectada.
- Modificar sus contraseñas, utilizando aquellas que sean seguras y distintas en todos los servicios en línea, desde el correo electrónico hasta el *homebanking*. Se debe evitar utilizar contraseñas con datos personales (nombres, apellidos, fechas, números de documento, teléfonos, etc.).

[26] Home Office Identity Fraud Steering Committee. 2006. http://www.identitytheft.org.uk/identity-crime-definitions.asp [18/02/2012]

- Descartar o destruir de una manera apropiada cualquier documentación con información personal. Una buena práctica es no arrojarlos a la basura, donde pondrían ser recogidos por un tercero.
- Disminuir al mínimo la información y documentación que se porta en billeteras y carteras.
- Solicitar un resumen a las compañías de informes crediticios para conocer el estado financiero de la persona afectada y detectar cualquier anomalía que pueda dar datos sobre el uso de la identidad por parte de terceros. En Argentina, la Ley Nº 25.326 de Protección de Datos Personales, garantiza el ejercicio del derecho al acceso a este informe en forma gratuita cada seis meses.
- Revisar cuidadosamente los resúmenes de cuenta y crediticios buscando cualquier anomalía en sus servicios y productos adquiridos.
- Controlar que los datos personales estén registrados correctamente en todos los sitios donde se encuentren almacenados y, en caso de detectar desviaciones, solicitar su corrección o eliminación.

Pasos posteriores al robo de identidad

En el caso de haber sido afectado por el robo de identidad o de sospecharlo, se deben realizar las siguientes acciones:

- De ser posible, conservar un registro con todos los detalles de los trámites y documentación relacionada con la persona afectada.
- Comunicar e informar de la situación a cualquier empresa que reclame actividades crediticias o financieras realizadas en nombre de la víctima y también a las organizaciones emisoras de documentación personal.
- Reportar y denunciar ante una entidad policial el robo de identidad o el uso de la misma por parte de terceros. En el caso de robo de identidad digital es conveniente informar a la organización que otorgaba el perfil virtual (correo electrónico, red social, foro, etc.)
- Elevar una “alerta de fraude” a las compañías de informes crediticios para que las mismas, en caso de ser consultadas por otras empresas de servicios, eviten que el delincuente continúe utilizando su identidad. Actualmente no existe un procedimiento normado sobre la forma de llevar adelante esta denuncia en cada compañía aunque, en todas ellas también debe solictarse un informe crediticio.
- En el caso de encontrar información crediticia perjudicial, disputar y corregir dicha información con las compañías involucradas, acción que es regulada por la Ley Nº 25.326.
- Intentar recuperar o, en su defecto, cerrar cualquier cuenta -real o virtual- que considere que haya sido comprometida por los delincuentes.
- Es importante contar con cualquier tipo documento físico que respalde la identidad del afectado: partidas de nacimiento, documentos físicos oficiales, denuncia policial relacionada, declaraciones juradas, disputas ante entidades crediticias o de servicios, etc.

Conclusiones

La identidad digital, entendida como el conjunto de rasgos y características particulares que una persona expresa a través de internet, forma parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral. Como se ha podido observar a lo largo del trabajo realizado, esta identidad digital está en situación de crisis, debido a los duros embates por parte de los ciberdelincuentes dedicados al robo y suplantación de identidades digitales. Entre las raíces de este delito, se encuentra una gran facilidad en la captación ilegítima de datos de identificación personal, inexistencia de legislación en la materia, falta de controles adecuados por parte de las entidades, así como los bajos niveles de educación en los usuarios de los servicios en internet, educación que es inversamente proporcional al nivel de uso de las redes sociales y telefonía movil.

El diagnóstico es claro y necesario, pero por sí solo no brinda ninguna herramienta para combatir este flagelo de internet. Por ello, y para finalizar la presente investigación, se considera apropiado aunar esfuerzos hacia el futuro, buscando la defensa de los usuarios afectados, buscando que se considere a la identidad digital como un bien jurídico protegido. En este sentido, proponemos la tipificación penal en Argentina del delito de **suplantación de identidad digital**, así como de la **tenencia y transferencia ilegítima de datos de identificación personal**.

A continuación, se deja el texto de la propuesta[27], no sin antes destacar que se considera que una adecuada legislación es parte de la solución, pero no una solución mágica. Junto con ella, deberá establecerse un centro de atención a las víctimas, con personal capacitado y con los recursos suficientes para poder, en la práctica, realizar una real persecución de estos delitos informáticos. Por último, insistir en que es fundamental la realización de campañas de capacitación y concientización a los usuarios con relación a buenas prácticas en materia de seguridad de la información.

> *ARTICULO 1º: Incorporase como Artículo 138 bis del Código Penal de la Nación el siguiente:*
>
> *Art. 138 bis: 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.*

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

Referencias Bibliográficas

MARTINEZ MEDRANO, Gabriel, "El robo de Identidad La responsabilidad de los Bancos y del Estado". 2007.http://tics.org.ar/index.php?option=com_content&view=article&id=36 [19/02/2012]

RUMMENS Joanna Ph.D, "Personal Identity and Social Structure in Sint Maartin/Saint Martin: a Plural Identities Approach". Unpublished Thesis/Dissertation: York University, pág. 157-159. http://canada.metropolis.net/events/ethnocultural/publications/identity_e.pdf [15/02/2012]

HOAR, Sean B., "Identity Theft: The Crime of the New Millennium". USA Bulletin, Marzo 2001. http://www.cybercrime.gov/usamarch2001_3.htm [15/02/2012]

GARTNER. "Gartner Says Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years", 9 de noviembre de 2006.

COMSCORE. "Latin America's Internet Population Grows 15 Percent in Past Year". 18 de marzo de 2011.

WISE DATA SECURITY. "Skimming: clonación de tarjeta de crédito". 26 de diciembre de 2011. http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html [15/02/2012]

THE GUARDIAN. "Twitter is harder to resist than cigarettes and alcohol, study finds". http://www.guardian.co.uk/technology/2012/feb/03/twitter-resist-cigarettes-alcohol-study [19/02/2012]

TURKLE, Sherry. "Identidad en Internet". 1994. http://biblioweb.sindominio.net/telematica/mud.html [20/02/2012]

MOLINA QUIROGA, Eduardo, "Los informes crediticios a diez años de la 25.326. Una visión crítica".

FEDERAL TRADE COMISSION (FTC). "Defiéndase contra el Robo de Identidad". http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/sidt04.pdf [20/02/2012]

SEGU-KIDS. Prevención del robo de identidad. http://www.segu-kids.org/padres/robo-identidad.html [20/02/2012]