2 EL DESAFÍO DE LA LUCHA CONTRA EL CIBERCRIMEN EN ARGENTINA

Marcelo Temperini

RESUMEN

El aumento en materia de delitos informáticos lleva consigo la aparición de diversas formas organizadas dedicadas al cibercrimen. En el presente artículo se pretende lograr un análisis sobre los principales desafíos en la lucha contra el cibercrimen en Argentina. El problema de las estadísticas; denuncias y cifra negra; centros de respuestas e investigación; la legislación adecuada; la necesidad de cooperación y colaboración, nacional e internacional; el incremento de la especialización de los ciberdelincuentes; entre otros, serán los tópicos planteados como elementos de una radiografía actualizada sobre el estado de situación en nuestro país.

PALABRAS CLAVE

cibercrimen, delitos informáticos, hacking, cracking, seguridad informática.

ABSTRACT

The rise in cybercrime entails the emergence of various forms dedicated to organized cybercrime. This article is intended to achieve an analysis of the main challenges of cybercrime fighting in Argentina. The problem of statistics, reports and black figure, responses and research centers, the challenge of appropriate legislation, the need for cooperation and collaboration, at the national and international level, the increase of the specialization of cybercriminals, among others, will be the topics raised as elements of an update in the state of affairs in our country radiography.

KEY WORDS

cybercrime, computer crime, hacking, cracking, information security.

«Siempre que vayas a atacar y a combatir, debes conocer primero los talentos de los servidores del enemigo, y así puedes enfrentarte a ellos según sus capacidades» (Sun Tzu, El arte de la guerra).

1. Introducción

Hace años que los delitos informáticos forman parte de la delincuencia en nuestra sociedad. El paso del tiempo genera los espacios necesarios para que el ciudadano tome conocimiento y dimensión de la existencia de este tipo de delitos. En este aspecto, algunos casos mediáticos han sido útiles para dar a conocer los distintos riesgos que implica la utilización de las redes de información. Casos como los cables diplomáticos y secretos difundidos por Wikileaks (*Clarín*, 30/07/2010), la aparición de Snowden (*Clarín*, 11/06/2013) y la apertura al mundo del programa de espionaje PRISM por parte de Estados Unidos, junto con otros tantos casos locales, van mostrando a la sociedad la existencia de una red de cibercrimen cada vez menos oculta.

En el presente artículo se pretende lograr un análisis sobre los principales desafíos que tenemos en materia de delitos informáticos en Argentina. Enj de 2013, la llamada Ley de Delitos Informáticos (Nº 26388),[1] cumplió cinco años desde su sanción en el país, lo que aparece como una oportunidad importante para realizar un balance sobre el estado de situación en la actualidad.

La finalidad de este trabajo será, entonces, realizar una radiografía actual de la problemática que representa el cibercrimen en nuestro país con el objeto de identificar y comprender los distintos desafíos que necesitamos superar para avanzar en políticas adecuadas para un real y eficaz combate contra la ciberdelincuencia.

2. El desafío de las estadísticas y los centros de respuestas

El primero de los desafíos a considerar resulta ser esencial para la adopción de políticas adecuadas por parte del Estado. Nos referimos a las estadísticas, un aspecto sustancialmente problemático en la materia, ya que hasta el momento no se conocen en Argentina estadísticas oficiales

1 Sancionada el 4 de junio de 2008.

que permitan observar y cuantificar los delitos informáticos ocurridos en nuestro territorio.

Este vacío implica dificultades para analizar seriamente el problema de la ciberdelincuencia en el país. La falta de estadísticas oficiales impide, por ejemplo, determinar qué tipo de delitos es el que prima, los bienes jurídicos más afectados, los objetivos de los delincuentes (empresas financieras, bases de datos personales, etc.), entre otros datos de interés que brindarían un marco adecuado para tomar decisiones de política criminal. A continuación, se desarrollarán los diversos temas relacionados con esta problemática.

2.1. Organismos oficiales

En Argentina, dependiente de la Jefatura de Gabinetes de Ministros, se ha creado el ICIC[2] (ex ArCERT), como el «Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad», mediante la Resolución JGM Nº 580/2011. El mismo tiene como finalidad

> impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran.

A fin de que los distintos estamentos gubernamentales puedan participar de dicho programa, el mismo establece la posibilidad de adhesión a través de unos formularios puestos a disposición en la Resolución de la Jefatura de Gabinete de Ministros Nº 3/2011. Es decir, dicho centro de respuestas (CERT) ha sido diseñado para recepcionar solamente aquellos reportes de incidentes de seguridad que ocurran en las redes del Sector Público Nacional.

Es útil destacar que el concepto de CSIRT/CERT[3] (Computer Emergency Response Team) fue inicialmente creado en 1988 por la Universidad de Car-

2 ICIC, Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

3 Un CSIRT es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece

negie Mellon como respuesta al gusano de Internet Morris.[4] Existen diferentes CERT públicos y privados en muchos países y, según FIRST[5] (Forum of Incident Response and Security Teams), la entidad que actualmente agrupa y coordina los CERT Internacionales, en Argentina existe un sólo CSIRT/CERT afiliado:[6] CSIRT-BANELCO para entidades bancarias privadas.

Entre los distintos objetivos determinados para ser llevados a cabo por el ICIC (de acuerdo con el art. 3 de la Resolución JGM Nº 580/2011), vale la pena destacar el inciso k y n, los cuales se detallan a continuación a efectos didácticos del lector:

> k) Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas del Sector Público Nacional que hubieren adherido al Programa y facilitar el intercambio de información para afrontarlos.
> n) Elaborar un informe anual de la situación en materia de ciberseguridad, a efectos de su publicación abierta y transparente.

Como puede advertirse en el inc. k, el ICIC se constituyó con el objetivo de gestionar los incidentes de seguridad ocurridos en los entes del Sector Público Nacional que hubieren adherido. Actualmente también se permite la adhesión de organizaciones civiles y del sector privado (art. 5), aunque no están claros los beneficios de dicha adhesión.

En cuanto al inciso n, puede advertirse la obligación por parte del ICIC de la publicación de un informe anual que, de forma «abierta y transparente» (texto propio de la norma), posibilita a todos los ciudadanos conocer el estado de situación en materia de seguridad informática de los entes del Sector Público Nacional. A más de dos años desde la creación del ICIC (julio de 2011), no se ha podido encontrar ningún informe publicado en virtud de la obligación impuesta por el citado inciso.

Más allá de estos incisos, y de manera general respecto de las funciones del ICIC, se destaca que el mismo no está destinado a recibir denuncias, algo que se han encargado de dejarlo claro y en letras mayúsculas en la publicación de la «Guía Práctica para realizar denuncias ante un posible

---

información que ayude a mejorar la seguridad de estos sistemas.

4 En noviembre de 1988, Morris fue el primer ejemplar de *malware* autorreplicable que afectó a Internet.

5 CERT miembros de FIRST en Argentina, http://www.first.org/members/map/ [consultado: 27 de noviembre de 2013].

6 A fecha 02/05/2013, según información brindada en FIRST. Url: http://www.first.org/members/teams [consultado: 27 de noviembre de 2013].

delito informático» (ICIC), en donde textualmente dice: «RECUERDE – EL ICIC no recibe denuncias. Asesora y recomienda».

En el asesoramiento realizado para el ciudadano víctima de delitos informáticos en la citada guía se pueden leer los siguientes pasos a seguir:

> 1. No borre, destruya, o modifique la información que posea en su computadora relacionada al hecho. Recuerde que siempre, la integridad de la información es vital para poder seguir adelante con las causas penales que se inicien.
> 2. Nunca reenvíe los mensajes (correos electrónicos) constitutivos del delito.
> 3. Realice inmediatamente realice la denuncia ante la dependencia policial más cercana a su domicilio (Comisaría de su barrio en cualquier lugar del país). Recuerden que tienen la obligación de tomar su denuncia.
> 4. A los fines de resguardar correctamente la prueba, una vez realizada la denuncia, proceda de la forma en que el investigador le indique.

El punto medular del asesoramiento se encuentra en el ítem 3: realizar la denuncia en la dependencia policial más cercana al domicilio de la víctima. Este aspecto, que puede ser considerado como simple, en una gran parte de nuestro país representa un problema en sí mismo, atento al desconocimiento y falta de capacitación que existe por parte de los agentes policiales.

En Santa Fe, por citar un caso difundido mediáticamente, un importante médico de la zona fue víctima de un caso de *hacking* (*UNO*, 05/08/2013). El Dr. Arturo Serrano (víctima) afirmó en varias entrevistas haber intentado denunciar ante diferentes comisarías sin lograr que en alguna de ellas le tomaran la denuncia por el hecho ocurrido.

2.2. La experiencia en el ámbito internacional

En países con mayor desarrollo, hace años que existen centros de respuesta para los casos de delincuencia informática. Por citar algunos, se pueden mencionar el IC3[7] de Estados Unidos, la UNEDEI[8] en México, la CYCO[9] en Suiza. Todos ellos, además de contar con una infraestructura

7 Internet Crime Complaint Center (IC3), en Estados Unidos fue establecido por una asociación entre el FBI y el NW3C (National White Collar Crime Center). Url: http://www.ic3.gov [consultada: 27 de noviembre de 2013].

8 Unidad Estatal de Delitos Electrónicos e Informáticos.

9 Cybercrime Coordination Unit Switzerland.

dedicada a la recepción de denuncias por parte de las víctimas, permiten que las propias denuncias puedan ser realizadas de forma electrónica (lo que admite el acceso al «sistema» de muchas más víctimas) e incluso en algunas de ellas se permiten las denuncias de tipo anónimo con el fin de fomentar a aquellos que han sido víctimas pero no quieren formar parte del proceso o bien desean reportar el incidente resguardando la confidencialidad de sus datos (un aspecto que posteriormente será tratado).

A nivel internacional, se debe destacar la Convención de Cibercriminalidad de Budapest, en cuyo art. 35 obliga a los Estados firmantes a la adopción de un Centro de Respuestas 24x7 a fines de determinar un punto de contacto de trabajo que haga factible la colaboración internacional en casos de cibercrimen.

2.3. Otras alternativas en estadísticas

Ante la inexistencia de estadísticas oficiales en la materia, podrá el lector válidamente preguntarse: ¿qué es lo que actualmente se utiliza para trabajar en materia de cibercrimen? A modo de respuesta preliminar, debemos reconocer que en la mayoría de los casos suelen utilizarse estadísticas realizadas por empresas privadas interesadas en el mundo de la seguridad de la información, tales como las publicadas por la empresa Symantec.

En el informe de la citada empresa, se afirma que los delitos informáticos producen una pérdida de 388 billones de dólares anuales (considerando el propio dinero robado más el dinero que les implica a las víctimas poder solucionar sus problemas), haciendo comparable cifras con la ocasionadas por el mercado negro de la marihuana y la cocaína, que es de 288 billones de dólares anuales.

Es legítimo preguntarse (y dudar) por la validez de dichas cifras, que son arrojadas a modo genérico y mundial, precisamente por una empresa cuyo negocio es la venta de una de las principales «armas» para defenderse de estos ataques informáticos (antivirus).

Por otro lado, desde una óptica más pública a nivel mundial, es posible citar el Comprehensive Study on Cybercrime[10] realizado por Naciones Unidas, en particular por la United Nations Office on Drugs and Crime (ONUDC), publicado en febrero de 2013 y en el cual se encuestó a más de 82 países, incluyendo varios de Latinoamérica (entre ellos, Argentina).

10 Naciones Unidas, New York, 2013. UNODC. Comprehensive Study on Cybercrimen.

Para la recopilación de información, la ONUDC elaboró un cuestionario que fue difundido entre los Estados miembros, las organizaciones intergubernamentales y las entidades del sector privado. Además, teniendo en cuenta la necesidad de equilibrar la representación de las diferentes regiones, se consultó a los representantes del sector privado, incluidos los representantes de los proveedores de servicios de Internet, los usuarios de los servicios y otros actores pertinentes, así como a representantes del mundo académico, de los países tanto desarrollados como en desarrollo.

Entre otros datos importantes que incorpora este estudio integral, se revela que en la mayoría de los países el índice de cibercriminalidad es notablemente más alto que los de los delitos tradicionales, tales como el robo o el hurto común. Mientras estos últimos tienen índices inferiores al 5 %, los delitos informáticos oscilan entre el 10 y el 17 %. Estos números pueden apuntalar con relativa facilidad las afirmaciones sobre el incremento de la delincuencia informática en los últimos años.

No obstante, y aun considerando que los delitos informáticos no reconocen límites de fronteras para su comisión (característica de este tipo de delitos), no se debe caer en la confusión de utilizar estadísticas generales de esta clase de estudios (realizados a nivel mundial) con las situaciones propias que vive cada país en particular.

3. El desafío de la falta de denuncias

En estrecha relación con el desafío anterior, se debe desarrollar la problemática de la propia falta de denuncias realizadas por las víctimas, que genera gran parte de la llamada «cifra negra» de los delitos informáticos.

De acuerdo con el Dr. Germán Aller (2006), la cifra negra es lo más próximo numéricamente a la cantidad real de crímenes cometidos en una sociedad determinada. La relación de tensión existente entre delitos realmente cometidos y los efectivamente tratados por el aparato penal engloba a la mayor cantidad de víctimas que ni siquiera serán atendidas, tratadas ni conocidas por el segmento penal, y a las cuales el Estado no da respuesta alguna. Según Aller, tal proceso «empuja» a las personas a no denunciar los actos ilícitos, a no reconocerse a sí mismas como víctimas y, en consecuencia, a la impunidad que el infractor penal asume, puesto que en el acto desvalorado no vislumbra un referente social acompasado del penal, en tanto a su conducta es delictiva, pero el núcleo social o persona

menoscabada por el delito que se ha cometido no pone en evidencia tal daño y, por ende, tampoco el segmento penal podrá operar en su contra.

Este autor señala que muchas víctimas no denuncian los delitos sufridos porque:

1. No se cree en la Policía ni en la justicia penal.
2. No se acepta la condición de víctima, debido a que implica pérdida de dignidad y falta de solidaridad.
3. No se quiere evidenciar la victimización individual ni colectiva.
4. El aparato penal carece de plataforma adecuada para abordar ni siquiera con un mínimo de éxito la solución del conflicto social base.
5. Se tiene miedo a la venganza o amenazas posteriores por parte del autor del delito.
6. Se quiere olvidar lo ocurrido.
7. Se desconoce que se haya cometido un delito.
8. La víctima se siente total o parcialmente culpable de lo sucedido.
9. Se ignora que puede pedir la intervención del Estado.

A simple vista, se pueden reconocer en el listado de causas realizado por el Dr. Aller, varios aplicables al ámbito del cibercrimen. Puntualmente, se tomarán algunas de ellas para un desarrollo personal sobre dichos aspectos.

a) *Falta de confianza en la Policía o la justicia:* en nuestro país, este aspecto es relevante en la mayoría de los casos, ya que existe un alto porcentaje de la población que tiene falta de confianza en la Justicia. Así lo demuestran desde hace años los estudios del Índice de Confianza en la Justicia[11] (ICJ) realizados por Fores, la Escuela de Derecho de la Universidad Torcuato Di Tella, y la Fundación Libertad. A marzo de 2010, los índices de confianza fueron del 50,5 % (en una escala donde 0 expresa el mínimo de confianza y 100 el máximo). El mismo estudio revela, por ejemplo, que en términos de eficiencia la Justicia en Argentina es poco confiable para el 55 % de los encuestados y nada confiable para el 22 % de la población consultada.

11 Foro de Estudios sobre la Administración de Justicia, «Índice de Confianza en la Justicia».

b) *El aparato penal carece de plataforma adecuada para abordar ni siquiera con un mínimo de éxito la solución del conflicto social base:* este punto, si bien tiene estrecha relación con el anterior, reviste sus diferencias. Puntualmente, es menester destacar que en muchos casos de delitos informáticos, para poder realizar una investigación eficaz tendiente a determinar y capturar al autor del mismo, es necesario poseer una infraestructura adecuada. Es decir, se precisa contar con los recursos técnicos necesarios, con personal disponible y capacitado, así como cierta agilidad en cuanto a coordinación y cooperación de distintos entes (relación ISP/Justicia). Estos aspectos en conjunto no suelen encontrarse (salvo excepciones) a lo largo de nuestro país, y aquí radica otra de las grandes problemáticas a ser abordadas.

c) *Se desconoce que se haya cometido un delito:* desde la experiencia en el trabajo privado de consultoría en seguridad informática, se puede afirmar que muchas personas que escriben para consultar por los problemas que han tenido en Internet desconocen totalmente que han sido víctima de un delito informático tipificado en Argentina. Esta falta de conocimiento por parte del promedio de la sociedad sobre la existencia de estos «novedosos» delitos hace que varios casos se pierdan dentro de la gran bolsa de la cifra negra.

Antes de finalizar, se considera oportuno agregar un elemento nuevo, o al menos una causa no considerada por el Dr. Aller que, desde la experiencia, se puede afirmar que es un aspecto decididamente relevante al momento de analizar la falta de denuncias sobre casos vinculados al cibercrimen.

d) *Confidencialidad como requisito:* muchas víctimas de distintos tipos de delitos informáticos deciden voluntariamente no denunciar sus casos, bajo el razonamiento que la posibilidad de difusión pública ocasionaría un daño peor al ya efectivamente sufrido. En este sentido, dentro del ámbito privado de la seguridad informática, una de las principales virtudes que analizará un cliente es precisamente el nivel de profesionalismo en cuanto a la confidencialidad de los casos. Dicha situación encuentra una lógica respuesta considerando que la víctima es consciente que de difundirse públicamente el incidente que ha sufrido (algo potencialmente probable en caso de denuncia ante las autoridades), su imagen, buen nombre, reputación, etc., podrían ser gravemente perjudicadas, superando ampliamente el daño ya recibido por el ataque informático en sí mismo.

A continuación se citan dos ejemplos para facilitar la comprensión de los lectores. Supongamos el caso de una importante empresa dedicada al rubro de la salud (clínica, en este caso), que es víctima de ataques informáticos que logran acceder a sus sistemas y hacerse con todas sus bases de datos, las cuales poseen información sensible sobre la salud de miles de personas de la región. La difusión de dicho incidente podría ocasionar daños irreparables en cuanto a la confianza de los clientes, construida con el trabajo de muchos años. Otro ejemplo puede ser un caso de un profesional reconocido en su ambiente (un periodista, un abogado, un psicólogo) que es víctima de un caso de interceptación de comunicaciones electrónicas (cuentas pinchadas) que hace posible que terceros extraños accedan a todas sus comunicaciones privadas (y eventualmente sean difundidas). Fácilmente puede advertirse que los daños ocasionados por una noticia (que vale destacar que es generalmente buscada atendiendo a la gran recepción que existe en la masa sobre este tipo de casos de problemas «cibernéticos») pueden ocasionar perjuicios irreparables, afectar bienes jurídicos de difícil reconstrucción (como la imagen, honor o reputación de una persona física o jurídica), comparativamente mucho más graves al daño ya sufrido.

4. El desafío de la internacionalización de los delitos informáticos

La internacionalización suele estar presente en la mayoría de los delitos informáticos, por lo que puede ser considerada como un aspecto esencial a tener en cuenta a la hora de trabajar sobre las políticas criminales que deben pensarse desde los Estados.

La internacionalidad como propiedad de los delitos informáticos implica que los mismos no encuentran barreras jurisdiccionales para llevarse a cabo. Es decir que, técnicamente es posible estar conectado a una red en Argentina, pasar por un *router*[12] conectado en Rusia, utilizar una *botnet*[13] de computadoras en Colombia y finalmente atacar un sistema en Cuba. Por más complejo que pueda parecer en el relato, técnicamente es de relativa facilidad, siempre que se cuente con un mínimo de conocimientos técnicos.

12 Un *router* o enrutador, es un dispositivo que proporciona conectividad a nivel de red.

13 Una *botnet* es una red de computadoras «zombies», es decir que han sido previamente infectadas y que permiten que quien tenga su control, pueda utilizarlas como armas para distintos tipos de ataques.

Estos casos vuelven a ponen sobre la mesa de los académicos las clásicas preguntas sobre la legislación aplicable, pero sobre todo evidencian el claro desafío de coordinar distintos ámbitos de colaboración internacional. Con relación a este último aspecto, el Convenio de Cibercriminalidad de Budapest[14] es el instrumento internacional más importante en la materia precisamente porque apunta a tener dentro de los Estados firmantes un mínimo de coordinación en el ámbito penal material y un potente marco de cooperación internacional (procesal penal) para casos de cibercrimen.

Argentina hace ya un tiempo que está en proceso de ingresar a dicho Convenio, pero de momento no es parte, ni existe fecha aproximada para su incorporación. En el importante caso de que sea aceptado, nuestro país tiene tareas pendientes en distintos aspectos que debe cumplimentar para formar parte de dicho grupo, especialmente en materia procesal penal.

Más allá de la ya citada necesidad de cooperación internacional, se considera de relevancia marcar la necesidad de un previo marco de cooperación nacional en Argentina. En la actualidad se pueden observar diferentes realidades en nuestro país, cada una de ellas dependiendo del grado de desarrollo o fortalece económica de cada provincia en particular (a modo de ejemplo, podría mencionarse que las víctimas en Buenos Aires tienen la posibilidad de denuncia ante la División de Delitos Tecnológicos de la Policía Federal Argentina o ante el Área Especial de Investigaciones Telemáticas de la Policía Metropolitana, opciones que no existen en la mayoría de las otras provincias de nuestro país).

Como consecuencia de la heterogeneidad de situaciones hacia el interior de Argentina, se propone considerar la necesidad de generación de una «Red Nacional de Cooperación en materia de Delitos Informáticos» para que aquellas provincias (como, por ejemplo, Santa Fe) que aún no tienen una estructura armada en la materia puedan acceder a los avances y experiencias de otras con mayor desarrollo en el área (tales como Buenos Aires y Córdoba), así como poseer canales ágiles de cooperación para los casos que requieran colaboración interjurisdiccional.

4.1. El desafío de la coordinación penal en Latinoamérica

Conforme a un reciente estudio de derecho comparado sobre delitos informáticos en Latinoamérica (Temperini, Delitos informáticos...), puede

14 Council of Europe. «Convenio de Cibercriminalidad de Budapest». Budapest, 23 de noviembre de 2001.

afirmarse que los más sancionados como tales a nivel latinoamericano son, por un lado, los delitos más clásicos (atentadoS contra la integridad de los datos y acceso ilícito) y, por otro, el delito relacionado a la pornografía infantil como contenido (difusión, comercialización, etc.), atendiendo a la importancia que representa la integridad de los menores como bien jurídico protegido.

Basados en este mismo estudio, se demuestra que los países latinoamericanos presentan un marcado cuadro de falta de homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos. Entre los principales factores para ello, se da el hecho de que dichos Estados han optado por diversas posturas político-criminales respecto de sus formas de regular, lo que como resultado una amplia gama de marcos penales.

Algunos de los países que formaron parte del estudio han optado por la sanción de leyes especiales, donde en los casos más destacados (caso de República Dominicana) incorporan conceptos propios, principios, parte penal material, parte procesal penal, e incluso a través de las mismas normas se han generado los organismos dedicados a su investigación y persecución. Otros tantos países (la mayoría) han optado por modificaciones parciales a sus Códigos Penales vigentes, adaptando las figuras penales clásicas a fin de que sea posible su aplicación en los delitos informáticos.

La falta de armonización a nivel regional observada en el estudio reconoce diferencias en dos niveles. En el primero de ellos se observan diferencias entre los países sobre los criterios políticos para la consideración sobre si tal acción lesiva debe ser o no sancionada como delito penal. En un segundo nivel, dentro de aquellos países que han dado respuesta positiva al primer nivel, se advierten diferencias en cuanto a los elementos y criterios penales considerados como necesarios para la configuración de un tipo penal en particular.

5. El desafío del Hacking as a Service (HaaS)

Según un estudio realizado por la empresa de seguridad informática McAfee[15] sobre las predicciones en materia de riesgos informáticos, el futuro está marcado por la aparición de una nueva gama de servicios: Hacking as a Service (HaaS). La proliferación de vulnerabilidades en los sistemas, combinada con un incremento de usuarios de escasos cono-

15 McAfee Labs, «Threats Predictions», 2013.

cimientos 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, etcétera.

Si bien la mayoría de los servicios que pueden ser encontrados en Internet para el usuario tradicional (búsquedas en Google) suele ser una estafa, también es posible encontrar otra gama de servicios más «profesionales», de personas de todas partes del mundo que, con ciertos conocimientos técnicos, encuentran en la delincuencia informática una manera de hacer dinero fácil a distancia. Dentro de la Deep Web[16] es factible encontrar una variedad de *crackers*[17] dispuestos a llevar a cabo una gran cantidad de delitos por la suma adecuada de dinero.

Según un estudio realizado por otra empresa de seguridad, Panda Security,[18] las mafias de ciberdelincuentes que operan en Internet están muy organizadas, tanto desde el punto de vista de visión estratégica como desde la operativa, logística y despliegue de sus operaciones. Además, no sólo pueden parecer verdaderas compañías sino que son organizaciones multinacionales, ya que operan a lo largo y ancho del planeta.

De este último informe, se ha extraído una clasificación publicada por el FBI acerca de las diferentes «profesiones» del mundo de los cibercriminales, en un intento por tipificar las figuras más comunes que podemos encontrar en el proceso mafioso de generar dinero mediante el robo, la extorsión y el fraude a través de Internet.

De acuerdo con el FBI, las organizaciones cibercriminales funcionan como empresas, cuentan con expertos para cada tipo de trabajo y ocupación. A diferencia de una organización empresarial, estos cibercriminales trabajan sin horarios, sin vacaciones y sin fines de semana. Entre las especializaciones más comunes que tipifica el FBI están las siguientes:

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

16 Deep Web es una importante parte de Internet cuyos contenidos no sin indexables, por lo tanto no es posible acceder a través de buscadores clásicos.

17 A fin de distinguir técnicamente los hackers (sentido positivo), los crackers son aquellas personas que utilizan sus conocimientos para realizar daños informáticos de distintos tipos.

18 Panda Security, «El mercado negro del Cibercrimen», 2010.

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.

Este estudio[19] indica que las organizaciones cibercriminales se organizan de forma jerárquica, y cada paso diferente de la cadena cuenta no con uno sino con varios especialistas.

Como se observa, existen distintos niveles o grados de profesionalización entre los delincuentes (como en muchos otros delitos) en materia de delitos informáticos. Por lo general, suele pensarse que los delincuentes informáticos actúan de forma aislada, espontánea, independiente, con distintas motivaciones. Sin embargo, el transcurso del tiempo y la experiencia en los delincuentes trae consigo la existencia de redes organizadas dedicadas a la comisión de delitos cada vez más complejos y la problemática está escalando en gravedad debido a la existencia de cada vez mayores redes internacionales dedicadas a este tipo de delitos.

Sobre estas bandas organizadas y relacionados con el delito de la comercialización de pornografía infantil a través de medios informáticos, se pueden citar en Argentina distintos casos de desbaratamientos de complejas redes. En 2013, por ejemplo, a través de la denominada «Operación Oliver»,[20] nacida bajo una investigación previa realizada en Londres. A

19 Op. cita 26

20 Secretaría de Comunicación Pública de la Presidencia de la Nación, «La Policía Federal desarticuló una red internacional de pornografía infantil»: http://prensa.argentina.ar/2013/01/11/37634-la-policia-federal-desarticulo-una-red-internacional-de-pornografia-infantil.php

través de la misma se realizaron 11 allanamientos en la ciudad de Buenos Aires, 24 en el conurbano bonaerense y 26 en distintas provincias (Salta, Tierra del Fuego, San Juan, Tucumán, Santa Fe, Santa Cruz, Córdoba, Santiago del Estero, Chaco, Entre Ríos y Neuquén), con la imputación de 64 personas involucradas.

6. El desafío de la legislación adecuada

En materia de derecho informático en general, es asumido que el derecho suele llegar bastante más tarde a los hechos que en otras ramas más tradicionales. Ello se debe, en principio, a que el avance de las nuevas tecnologías es más vertiginoso que otros aspectos de nuestra sociedad (familia, laboral, etc.) y genera una dinámica a la que el mundo jurídico no está acostumbrado.

En este contexto, se producen situaciones de propuestas, proyectos o discusiones que pueden durar años y que cuando finalmente son reguladas (bajo alguna postura) por el derecho, dichas regulaciones se encuentran desactualizadas. De allí se debe destacar la vital importancia de una adecuada técnica legislativa al momento de proyectarse algún tipo de normativa que tenga por destino la regulación de las nuevas tecnologías.

Desde el ámbito penal de los delitos informáticos, es necesario considerar que, una vez penalizada cierta actividad, los delincuentes buscan adaptarse a los distintos ambientes, realizan aquello que no estaba previsto o elaboran nuevas técnicas a partir de la creatividad e innovación para terminar ejecutando acciones que aprovechan deficiencias técnicas y legales de la normativa vigente.

Como ejemplo, citamos el caso de la tipificación del *phishing*[21] en Argentina. El mismo había sido incorporado por el art. 9 de la Ley Nº 26388. Es decir, fue incorporado a través del inciso 16 del art. 173, el cual regula los tipos especiales de la estafa del art. 172 (tipo penal básico de estafa).[22]

21 Phishing es un término para definir un tipo de abuso informático que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

22 Ley Nº 26388 - Artículo 9º — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Recurriendo a la doctrina clásica penal del delito de estafa, para así saber cuando quedará configurado el tipo, citamos la impecable explicación de Edgardo Donna, quien afirma que

> es importante aclarar que en la estafa el bien jurídico no es, como podría pensarse, la «buena fe en el tráfico» o la «lealtad en las operaciones» sino el patrimonio. El ardid y engaño previstos en el tipo como formas de comisión constituyen simplemente los medios con los que se produce el daño patrimonial del sujeto pasivo, de modo que el quebrantamiento de la buena fe es el *modus operandi* que va a determinar la lesión jurídica patrimonial, pero no el objeto de la tutela, ni directa ni indirectamente. Si la buena fe fuese el bien jurídico amparado, la consumación del delito debería producirse con la sola realización del engaño, sin necesidad de que ocasione perjuicio patrimonial alguno, solución que resulta inaceptable desde el punto de vista legal (Donna y Fuente, 2000:57).

En conclusión, para que quede configurado el delito de estafa (y por lo tanto el caso especial propuesto en el inc. 16 para el *phishing*), debe existir primero el ardid o engaño y luego un perjuicio patrimonial consecuencia de dicho engaño. De aquí se puede deducir que el *phishing* en realidad no está penalmente tipificado en Argentina, al menos no hasta que en dichas acciones exista un perjuicio patrimonial que permita la aplicación del tipo de estafa, algo que en una gran parte de los casos de *phishing* de cuentas privadas (mails, redes sociales, etc.) nunca sucederá.

Lo que se puede inferir de modo general, dado que la complejidad del tema merece un desarrollo propio que se ha realizado en otras ocasiones (Temperini, 2011), es que en realidad lo que se terminó tipificando a través del citado artículo 173 inc. 16 de la norma argentina es un caso de estafa informática. No obstante, el tipo penal adolece de otros grandes problemas técnicos para su aplicación práctica, por lo que termina siendo aplicado el tipo básico de estafa.

En el caso de intentar tipificar el *phishing*, se debe considerar que el bien jurídico a proteger no es el patrimonio sino la información y, más precisamente, su confidencialidad. El autor de este artículo ha contado con la oportunidad de proponer un Proyecto de Ley para la tipificación de la «Captación Ilegítima de Datos Confidenciales» (*phishing*). El mismo ha sido presentado en el Honorable Senado de la Nación Argentina, bajo el Nº de Expediente S-2257/11, a través de la senadora nacional María de los Ángeles Higonet. Dicho proyecto de ley, junto con otro proyecto en el cual también se ha participado de su redacción (destinado a la tipificación

de la Suplantación de Identidad Digital) han sido oportunamente defendidos en la Comisión de Justicia y Asuntos Penales del Senado de la Nación.

Más allá del caso puntual del *phishing* en nuestro país, que a los fines del presente trabajo tiene más un efecto ejemplificador que otra cosa, a modo general y de cierre del presente desafío se debe considerar la necesidad de un importante trabajo a nivel legislativo para que, sin caer en la generación de una multiplicidad de tipos penales inútiles para la práctica (con el consecuente problema de la expansión penal), se disponga de una legislación adecuada, técnica y jurídicamente, que realmente sea eficaz para combatir el cibercrimen.

7. Conclusiones

Como se ha podido observar a lo largo del trabajo, el estado de situación actual en materia de cibercrimen presenta variados y complejos desafíos que deben ser seriamente analizados a fin de buscar alternativas para su superación o, al menos, su mitigación.

La falta de estadísticas oficiales en Argentina es un serio problema que debe ser abordado tan pronto como sea posible para que, dentro de un plazo razonable, se pueda contar con un diagnóstico real sobre la situación en el país.

Se destaca además la relación de esta problemática con la inexistencia de organismos o dependencias dedicadas a la recepción de denuncias y asesoramiento de las víctimas de delitos informáticos, independientemente del lugar en que se encuentren (sistema o red pensado sobre un sistema federal).

Argentina debería contar con un Centro de Atención de Respuestas 24x7 (en coincidencia con las recomendaciones internacionales) que cuente con recursos humanos capacitados y los recursos técnicos necesarios para ejecutar las tareas de asesoramiento, recepción de denuncias e investigación y, en los casos que correspondan, ejecutar la derivación de las denuncias con las autoridades locales adecuadas, de acuerdo con el domicilio de la víctima.

El desafío de la falta de denuncias por parte de las víctimas (cifra negra) debe ser abordado a través de la difusión y concientización de la problemática a nivel social, combatiendo las principales causas: falta de confianza en la Policía y en la justicia; el hecho de que el aparato penal carezca de plataforma idónea para abordar ni siquiera con un mínimo de éxito la solución del conflicto social base; el desconocimiento de que se haya cometido un delito.

La necesidad de considerar la «confidencialidad como requisito» en la lista de causas de la cifra negra se hace imprescindible, con el razonamiento y la experiencia de que la difusión pública del incidente informático puede ocasionar a la víctima serios perjuicios (por estar afectados bienes jurídicos de dificil reconstrucción, tales como la imagen, honor o reputación), los cuales en determinados casos pueden ser un daño considerablemente mayor al ya sufrido en el propio delito informático.

El incremento observado sobre la oferta de servicios ilegales ofrecidos en Internet, bajo la modalidad de Hacking as a Service (HaaS), donde es posible encontrar una variada gama de *crackers* dispuestos a realizar distintos tipos de delitos informáticos a cambio del precio adecuado, es una problemática que también debe ser abordada a fin de contener la ramificación de las bandas dedicadas al cibercrimen.

Se requiere considerar la especialización creciente en las bandas organizadas, acentuando la división de tareas en distintos tramos de delitos complejos, donde los niveles de riesgos asumidos por parte de delincuentes corresponden con las correlativas ganancias.

En cuanto al desafío de la coordinación penal, se destaca la necesidad de mejorar los niveles de armonización, coordinación y actualización legislativa en la materia, tanto a nivel nacional como regional (latinoamericano), con la finalidad de mitigar la existencia de «paraísos legales» que favorezcan los asentamientos de bandas dedicadas a la ciberdelincuencia.

A nivel nacional, se deja constancia sobre la heterogeneidad de situaciones hacia el interior de nuestro país, por lo que se propone considerar la necesidad de generación de una «Red Nacional de Cooperación en materia de Delitos Informáticos», con el objeto de que aquellas provincias que aún no tienen una estructura armada en la materia puedan acceder a los avances y experiencias de otras con mayor desarrollo, incentivando así la generación de canales ágiles para los casos nacionales que requieran colaboración interjurisdiccional.

A modo de reflexión final sobre lo trabajado, se concluye que el estado de situación en Argentina con relación a la lucha contra el cibercrimen, presenta variados y diversos desafíos. La sanción de la llamada Ley de Delitos Informáticos debe ser un puntapié inicial y un fin en sí mismo.

La superación o mitigación de estos desafíos involucra aspectos técnicos, jurídicos, socioculturales y políticos que requieren de un abordaje responsable e interdisciplinario por parte del Estado, basado en la previa comprensión y dimensionamiento de la problemática que implica el cibercrimen en Argentina.

Referencias bibliográficas

ALLER, Germán (2006). Cuestiones Victimológicas de Actualidad: Origen de la Victimología, Seguridad, Cifra Negra, Personalización del Conflito y Proceso Penal. Revista *ILANUD* N° 27.

COUNCIL OF EUROPE. *Convenio de Cibercriminalidad de Budapest*. Budapest, 23 de noviembre de 2001. Disponible en: http://www.coe.int/t/dghl/standardsetting/tcy/ETS_185_spanish.pdf [consultado: 27 de noviembre de 2013].

CYBERCRIME COORDINATION UNIT SWITZERLAND (CYCO). Disponible en: http://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html [consultado: 27 de noviembre de 2013].

DIARIO *CLARÍN* (11/06/2013). Hackeamos a cualquiera en cualquier parte del mundo. Disponible en: http://www.clarin.com/mundo/Hackeamos-cualquier-parte-mundo_0_935906490.html [consultado: 27 de noviembre de 2013].

DIARIO *CLARÍN* (30/07/2010). La Casa Blanca implora a WikiLeaks que no filtre más documentos sobre la guerra. Disponible en: http://www.clarin.com/mundo/Casa-Blanca-implora-WikiLeaks-documentos_0_307769448.html [consultado: 27 de noviembre de 2013].

DIARIO *UNO* (05/08/2013). Hackearon el mail de un santafesino para estafar a sus contactos. Disponible en: http://www.unosantafe.com.ar/santafe/Hackearon-el-mail-de-un-santafesino-para-estafar-a-sus-contactos-20130805-0018.html [consultado: 27 de noviembre de 2013].

DONNA, Edgardo y FUENTE, Esteban Javier (2000). *Aspectos generales del tipo penal de estafa.* Revista de Derecho Penal, N° 2000-2. Santa Fe: Rubinzal-Culzoni.

FORO DE ESTUDIOS SOBRE LA ADMINISTRACIÓN DE JUSTICIA. *Índice de Confianza en la Justicia.* Disponible en: http://www.foresjusticia.org.ar/investigacion-detalle.asp?IdSeccion=17&IdDocumento=68&idcategoria=22 [consultado: 27 de noviembre de 2013].

ICIC. *Guía Práctica para realizar denuncias ante un posible delito informático*. Disponible en: http://www.icic.gob.ar/archivos/instructivo_denuncias.pdf [consultada: 27 de noviembre de 2013].

INTERNET CRIME COMPLAINT CENTER (IC3). En Estados Unidos fue establecido por una asociación entre el FBI y el NW3C (National White Collar Crime Center). Disponible en: http://www.ic3.gov [consultado: 27 de noviembre de 2013].

MCAFEE LABS (2013). *Threats Predictions*. Disponible en: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf [consultado: 27 de noviembre de 2013].

NACIONES UNIDAS (2013). UNODC. *Comprehensive Study on Cybercrimen*. Disponible en: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf consultado: 27 de noviembre de 2013].

PANDA SECURITY (2010). *El mercado negro del Cibercrimen*. Disponible en: http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf [consultado: 27 de noviembre de 2013].

PANDA SECURITY (2010). *El mercado negro del Cibercrimen*. Disponible en: http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf [consultado: 27 de noviembre de 2013].

SECRETARÍA DE COMUNICACIÓN PÚBLICA DE LA PRESIDENCIA DE LA NACIÓN. *La Policía Federal desarticuló una red internacional de pornografía infantil*. Disponible en: http://www.prensa.argentina.ar/2013/01/11/37634-la-policia-federal-desarticulo-una-red-internacional-de-pornografia-infantil.php [consultado: 27 de noviembre de 2013].

SYMANTEC (2011). *Norton Cybercrime Report 2011*. Disponible en: http://www.symantec.com/content/en/us/home_homeoffice/html/ncr/ [consultado: 27 de noviembre de 2013].

TEMPERINI, Marcelo. *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.* 1ra. Parte. Publicado en el 1er. Congreso Nacional de Ingeniería Informática y Sistemas de Información.

TEMPERINI, Marcelo (2011). Phishing: Tipo penal en Argentina y sus consecuencias. *Segu-Info*. Disponible en: http://blog.segu-info.com.ar/2011/02/phishing-tipo-penal-en-argentina-y-sus.html#axzz1rdt8VTWf [consultado: 27 de noviembre de 2013].

UNIDAD ESTATAL DE DELITOS ELECTRÓNICOS E INFORMÁTICOS. Fiscalía General de Chihuahua, México. Disponible en: http://fiscalia.chihuahua.gob.mx/intro/?page_id=3029 [consultado: 27 de noviembre de 2013].

Marcelo Temperini

Abogado, especializado en Derecho Informático. Codirector de la Fundación ElDerechoInformático.com. Doctorando Conicet en investigación de Delitos Informáticos y Cibercrimen en el Centro de Investigaciones (FCJS–UNL). Prosecretario en la Comisión Derecho Informático y Nuevas Tecnologías del Colegio Público de Abogados de Santa Fe, 1ra. Circunscripción Judicial. Vocal titular y miembro de la Asociación de Derecho Informático de Argentina (ADIAr). Técnico analista de seguridad y vulnerabilidad de Redes de Información. Socio fundador de AsegurarTe, empresa de Consultoría y Gestión de la Seguridad de la Información. Responsable del Departamento de Investigación y Desarrollo. Colaborador de la iniciativa del Observatorio Iberoamericano de Protección de datos.

———

REGISTRO BIBLIOGRÁFICO

Marcelo Temperini

«EL DESAFÍO DE LA LUCHA CONTRA EL CIBERCRIMEN EN ARGENTINA», en *Papeles del Centro de Investigaciones*, Facultad de Ciencias Jurídicas y Sociales, UNL, publicación semestral, año 5, número 16, Santa Fe, República Argentina, 2015, pp. 31–51.