La cifra negra de los delitos informáticos: Proyecto ODILA

Abog. Marcelo Temperini[1], Lic. Cristian Borghello[2], AIA Maximiliano Macedo[3]

Abstract en Español. Los delitos informáticos ya dejaron de ser un problema a futuro para convertirse en un problema del presente. De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. Una problemática que no distingue entre víctimas, siendo un delito de tipo pluriofensivo, viéndose afectada la confidencialidad, integridad y disponibilidad de la información, así como la privacidad, el patrimonio, la reputación e imagen de las personas, entre otras. La cifra negra existente, es consecuencia de la falta de estadísticas oficiales en la materia, representando un aspecto sustancialmente problemático que impide desarrollar un trabajo serio de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el cibercrimen. En este marco, se propone la creación del Observatorio Latinoamericano de Delitos Informáticos: ODILA. Este proyecto, busca construir un espacio de investigación y trabajo en materia de delitos informáticos, especialmente dedicado a relevar y recolectar información sobre delitos informáticos ocurridos en Latinoamérica, con la finalidad de generar, sistematizar y difundir información sobre la realidad de esta problemática, así como fomentar la realización de denuncias por parte de las víctimas.

Keywords: delitos informáticos, cibercrimen, cifra negra, estadísticas, latinoamérica, ODILA

1. Introducción

De acuerdo a un informe [1] elaborado por la empresa Symantec, las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo por supuesto a América Latina. En las estadísticas citadas, las víctimas de los delitos informáticos aumentaron de un 10% a un 13% sólo entre el año 2011 a 2012. Tal como expresa Nir Kshetri en una de sus obras [2], "*El crecimiento meteórico del cibercrimen ha sido un tema de preocupación apremiante para nuestra sociedad*"[4]

Los delitos informáticos ya dejaron de ser un problema a futuro para convertirse en un problema del presente. De acuerdo a diferentes estudios actuales, los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez mayor. Una problemática que no distingue entre víctimas, siendo un delito de tipo pluriofensivo, viéndose afectada la confidencialidad, integridad y disponibilidad de la información, así como la privacidad, el patrimonio, la reputación

---

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

2 Licenciado en Sistemas con Certificaciones Internacionales en Seguridad de la Información. Director de Segu-Info y Segu-Kids. cborghello@segu-info.com.ar

3 Analista en Informática Aplicada (FICH-UNL). Socio Fundador de AsegurarTe – Consultora en Seguridad de la Información.

4 Traducción propia, originalmente el autor expresó *"The meteoric rise in cybercrime has been an issue of pressing concern to our society"*.

e imagen de las personas, entre otras. La cifra negra existente, es consecuencia de la falta de estadísticas oficiales en la materia, representando un aspecto sustancialmente problemático que impide desarrollar un trabajo serio de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el cibercrimen. En este marco, se propone la creación del Observatorio Latinoamericano de Delitos Informáticos: ODILA. Este proyecto, busca construir un espacio de investigación y trabajo en materia de delitos informáticos, especialmente dedicado a relevar y recolectar información sobre incidentes o delitos informáticos ocurridos en Latinoamérica, con la finalidad de generar, sistematizar y difundir información sobre la realidad de esta problemática.

2. El concepto de delito informático

Entre las distintas precisiones que son necesarias de realizar, es necesario adelantar al lector que la variedad de denominaciones para los delitos por un lado, sumado a la multiplicidad de formas de criminalización de las conductas analizadas que se dan en los distintos países incluidos en el estudio, representan un importante desafío al momento de lograr un consenso sobre cuáles son los llamados "delitos informáticos".

A fines de adoptar un criterio para la construcción de estas categorías, tomamos el concepto de delito informático desarrollado por el Dr. Julio Tellez Valdes [3], quien los clasifica en sus formas típica y atípica, entendiendo por la primera a "*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*" y por las segundas "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"*. Si bien existen otros tantos conceptos en la doctrina, tomamos el citado toda vez que su simple clasificación entre típicos y atípicos es útil a los fines de este trabajo. Aquí, solamente consideraremos como "delito informático" a aquellos dentro de las categorías de los típicos, es decir, como una conducta penalmente sancionada.

Ahora, en un segundo escalón de razonamiento del "delito informático", se plantea una decisión que dependiendo de la postura, los delitos informáticos son algunos pocos o se multiplican de una forma considerable. Nos estamos refiriendo a que en por lo general, el concepto de "delito informático" está reservado para aquellos tipos penales específicos de la materia (por ejemplo, casos de hacking, cracking, denegación de servicios, etc.). Sin embargo, de acuerdo a una interpretación taxativa del concepto ya descripto, si la conducta típica se realiza a través de un medio informático o telemático (*nos parece más correcto que mencionar "computadoras" como se expone en el concepto original*), también pasaría a ser un delito informático... ¿Es esto correcto?

El autor Miguel Angel Davara Rodríguez [4] define el delito informático como "la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software". Agregando luego: "Nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General".

A nuestro parecer, la respuesta es positiva y negativa a la vez. Es decir, es cierto que la mera intervención de un elemento informático, no convierte a un delito clásico en un delito informático. Sin embargo, es necesario reconocer que en

determinados tipos penales, el ingrediente tecnológico es tan poderoso, que por un lado hace necesario que para su persecución y sanción, intervengan especialistas dedicados a los delitos informáticos, y por otro, el hecho en sí, termina padeciendo de muchos de los inconvenientes o desafíos clásicos de los delitos informáticos, tales como el anonimato, internacionalidad, dificultad en la obtención de evidencia digital, entre otros.

A modo de comparación, similar situación se da con otros delitos de los cuáles pocos dudan de su verdadera condición de "delitos informáticos". Estamos hablando de los casos de la estafa electrónica y de la pornografía infantil. Ambos flagelos datan de muchísimos años antes que existiera Internet o las llamadas nuevas tecnologías si queremos ser más inclusivos. Sin embargo, ha sido necesario adaptar ambas figuras penales, precisamente porque la combinación de las nuevas tecnologías al momento de atacar los mismos bienes jurídicos (patrimonio por un lado, integridad sexual de los menores en el otro), pusieron en evidencia la potencialidad de daño de llevarse a cabo estos delitos clásicos a través de medios informáticos o telemáticos.

En la práctica, gran parte de las personas víctimas de problemas relacionados con Internet y las nuevas tecnologías, terminan recurriendo a especialistas en Seguridad de la Información, a fin de obtener algún tipo de solución alternativa a sus problemas (acosos a través de perfiles falsos, injurias anónimas por correo electrónico, entre otros) precisamente porque no encuentran en el Estado, algún tipo de respuesta satisfactoria ante la vulneración de sus derechos.

Es importante destacar esto, porque en definitiva termina siendo el fundamento de porqué si bien las injurias o amenazas no son técnicamente "delitos informáticos", si hemos decidido incorporarlos entre las distintas opciones de "hechos" que pueden ser elegidos por los usuarios al momento de informar su reporte.

Por último, y antes de pasar a un desarrollo más pormenorizado de distintos desafíos que plantean los delitos informáticos, nos parece atinado citar al Dr. Horacio Fernández Delpech [5], quien en su última obra realiza un detalle sobre serie de circunstancias que hacen que este tipo de ilícitos penales sean de difícil represión:

1) La falta de una tipificación específica en la mayoría de las legislaciones de los delitos informáticos y cometidos a través de la red;
2) La trasnacionalidad de las conductas, que muchas veces se realizan en un país, pero cuyos resultados se producen en otro;
3) La falta de consenso internacional sobre la reprochabilidad de ciertas conductas;
4) Las permanentes innovaciones tecnológicas, que generalmente avanzan más rápido que las implementaciones de soluciones normativas;

3. El problema de las estadísticas

Si bien al comenzar el artículo, citamos una de las estadísticas más reconocidas en el ámbito de la seguridad de la información, debemos realizar algunas consideraciones que consideramos pertinentes en relación a lo que consideramos como el problema (o desafío) de las estadísticas en materia de cibercriminalidad.

La falta de estadísticas oficiales en la materia, es al menos para estos autores, un aspecto sustancialmente problemático, toda vez que ello impide un trabajo serio de

observación, análisis y elaboración de estrategias o planes orientados a combatir el cibercrimen.

Hasta el momento, no se conocen en Argentina (ni en América Latina) estadísticas oficiales generales que permitan observar y cuantificar los delitos informáticos ocurridos en todo nuestro territorio.

En nuestro país, es posible citar un importante esfuerzo llevado adelante por el Dr. Ricardo Sáenz [6], Fiscal General ante la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, que en el año 2010 ha llevado adelante un estudio solicitando a las Fiscalías Criminales y Correccionales Federales de todo el país, Fiscalías Nacionales en lo Criminal de Instrucción, Fiscalías Correccionales y Fiscalías de Menores que informaran la cantidad de causas iniciadas con motivo de la sanción de la ley 26.388 hasta el 30 de junio del año 2010 .

En ese informe se requirió, asimismo, que comunicaran: el modo de inicio de las actuaciones (prevención, denuncia en cámara, denuncia en fiscalía, denuncia en sede policial, denuncia remitida desde el extranjero), si el trámite de la causa se encontraba delegado en la fiscalía, si el autor era conocido o tramitaba como NN; cuáles eran los delitos investigados; las dificultades más relevantes ya fueran técnicas o jurídicas en la investigación de esos delitos; el cuerpo técnico interviniente y, por último, la proyección internacional de los delitos informáticos y los obstáculos más significativos relacionados con esa cuestión.

De acuerdo a este estudio, los delitos más denunciados en esa etapa, fueron en primer lugar las estafas informáticas (art. 173 inc. 16), seguido por casos de pornografía infantil (art. 128) y finalmente en tercer lugar los casos de acceso ilegítimo (ar.t 153). Entre las conclusiones de dicho trabajo, se destaca lo siguiente:

"Enfocarnos únicamente en los delitos informáticos previstos en la ley 26.388 nos confirmó que, aunque existe un número elevado de casos en los que interviene la justicia penal, aún existe un gran número que tenemos que incluir dentro de la cifra negra de esta clase de delitos. En nuestra opinión, esta situación responde a la falta de conocimiento general en lo que a este tema se refiere, así como también a la carencia de normas que castiguen las nuevas conductas que revisten características suficientes como para incluirlas como accionares ilícitos."

"El relevamiento pone en evidencia, sin lugar a dudas, que la capacitación de los operadores de la justicia es indispensable para una mejor y más cabal comprensión de la ciberdelincuencia en todos sus aspectos legales. Las particularidades que esta nueva forma de delincuencia reviste presenta serias dificultades investigativas: la transnacionalidad del accionar ilícito pone en juego a los principios básicos de la ley penal aplicable; el anonimato atenta contra la efectividad en la identificación de los ciberdelincuentes; el ciberdelito se perpetra en cuestión de segundos y la evidencia digital que prueba su comisión y permite un primer rastreo de los datos que nos conduzcan a la obtención de información que de fundamento al inicio de la pesquisa, se elimina, se altera y se pierde, sin que pueda ser recuperada, en la mayoría de las veces, con la misma velocidad."

Este trabajo, fue de vital importancia para la creación del Equipo Fiscal Especializado en Delitos y Contravenciones Informáticas, que actúa con competencia única en toda la Ciudad Autónoma de Buenos Aires, con el fin de investigar los delitos informáticos propiamente dichos, y aquellos que se cometen a través de internet que por su complejidad en la investigación o su dificultad en individualizar a los autores, merecen un tratamiento especializado.

Dicho equipo, fue generado el 15 de noviembre de 2012, donde la Fiscalía General de la CABA dictó la Resolución 501/12, a través de la cual, creó como

prueba piloto por el término de un año, el Equipo Fiscal Especializado en Delitos y Contravenciones Informáticas. A finales de 2013, dicho equipo (compuesto por Daniela Dupuy, Tomás Vaccarezza, Mariana Kiefer y Catalina Neme, entre otros), ha publicado un informe sobre el trabajo realizado durante el primer año de funcionamiento.

Estadísticas de casos ingresados

GRÁFICO 1: Ingreso de casos periodo 15 de noviembre de 2012 a octubre 2013

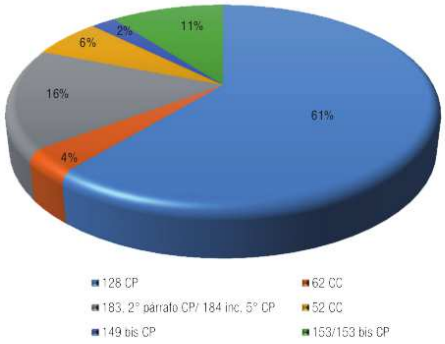
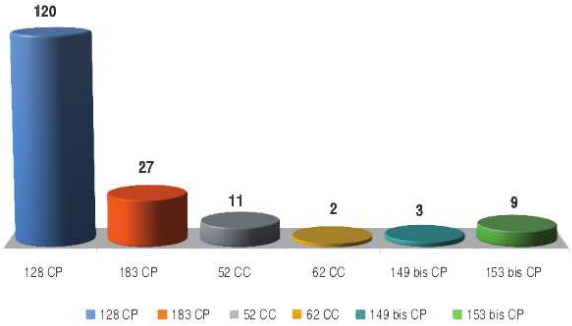


GRÁFICO 2: Resolución de casos

GRÁFICO 3: Casos en trámite al día de la fecha



Antes de sacar algún tipo de conclusiones sobre estas estadísticas, es necesario mencionar que dicho equipo de trabajo no posee competencia sobre todo tipo de delitos informáticos, sino solamente sobre aquellos que expresamente se han delimitado, a fin de que la tarea del grupo no se encuentre desbordada (más aún en consideración de su intención de conformación como prueba piloto). Como puede observarse de los gráficos, estos delitos solamente son: Pornografía Infantil (art. 128 CP); Daño informático y daño agravado (art. 183 2do párrafo y art. 184 inc. 5to. CP), Amenazas (art. 149 bis CP); Hostigamiento, maltrato o intimidación (art. 52 Cód. Contravencional de CABA[5]); Suministro de material pornográfico a menores (art. 63 Cód. Contravencional de CABA[6]).

Entre las conclusiones de dicho informe, se destaca *"el incremento incesante de casos informáticos a la justicia local, el que ha superado ampliamente las*

5 r. Quien intimida u hostiga de modo amenazante o maltrata físicamente a otro, siempre que el hecho no constituya delito, es sancionado con uno (1) a cinco (5) días de trabajo de utilidad pública, multa de doscientos ($ 200) a un mil ($ 1.000) pesos o uno (1) a cinco (5) días de arresto. Acción dependiente de instancia privada.

6 Ley 1473 CABA - Artículo 62 - Suministrar material pornográfico. Quien suministra o permite a una persona menor de dieciocho (18) años el acceso a material pornográfico es sancionado/a con uno (1) a cinco (5) días de trabajo de utilidad pública, doscientos ($ 200) a un mil ($ 1.000) pesos de multa o un (1) a cinco (5) días de arresto. La sanción se eleva al doble en caso que tal conducta se dirija a una persona menor de dieciséis (16) años. Admite culpa.

expectativas iniciales. Nótese que actualmente contamos con ciento setenta y dos (172) casos de delitos informáticos en trámite, sin perjuicio que, además, investigamos otros doscientos cuarenta y cuatro (244) delitos y contravenciones comunes; lo que eleva a un total de cuatrocientos dieciséis (416) casos los absorbidos por este equipo fiscal. Asimismo, varios son los factores que justifican considerar que el ingreso de casos va a aumentar significativamente en un futuro inmediato".

Como comentábamos inicialmente, lo publicado en el citado informe, son las únicas estadísticas oficiales existentes, que sólo hacen referencia a un determinado conjunto de delitos, y sobre casos exclusivamente de la Ciudad Autónoma de Buenos Aires. Es decir, no existen estadísticas o cifras que permitan observar la magnitud de la problemática que representan los delitos informáticos a nivel nacional, o al menos, provincial.

Este vacío implica diversas 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 son los más cometidos, los bienes jurídicos más afectados, determinar los tipos de objetivos de los delincuentes (empresas financieras, bases de datos personales, etc.), entre otros datos de interés que brindarían un marco adecuado para tomar determinadas decisiones de política criminal.

4. Estadísticas corporativas e internacionales

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, citadas al comienzo de este artículo.

En el informe de la citada empresa, se afirma que los delitos informáticos producen una pérdida de 388 mil millones 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 mil millones 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, *firewall* y otras herramientas similares).

En un estudio sobre cibercrimen encargado por la Organización de Estados Americanos [7], se reconoció que el cibercrimen ha crecido (entre 2011 y 2012) entre el 8 a 12 % en algunos países, y en el caso más extremo, de cerca del 40%. Más allá de la estadística, y en relación a la propia problemática de la recolección de datos que permitan analizar el estado de situación, el estudio afirma que "o*bviamente, los incidentes cibernéticos incluidos en los informes de los gobiernos de los Estados miembros de la OEA representan solamente una fracción del número total de incidentes y otras formas de delincuencia cibernética que se llevan a cabo en la región. Pero* ***sigue siendo sencillamente imposible en este momento recopilar datos que permitan obtener una imagen verdaderamente exhaustiva y detallada de la extensión de todos estos incidentes y actividades en las Américas y el Caribe****, o en cualquier otro sitio. Como ya dijimos, el intercambio de información dentro de los gobiernos —incluso aquellos con la capacidad más avanzada en materia de seguridad cibernética— sigue quedando corto, en gran parte debido a*

las realidades prácticas de que múltiples organizaciones tengan que responder simultáneamente a una gama de amenazas y blancos en constante evolución. Y muchas empresas privadas y otras entidades no gubernamentales siguen mostrándose reacias a reportar ataques o violaciones. ***Contabilizar el número de incidentes que afectan a los ciudadanos individuales plantea un desafío incluso mayor, en vista del porcentaje incluso más alto de ellos que pasan desapercibidos y no se reportan. Por último, la falta de colaboración generalizada y persistente entre las partes interesadas en todos los niveles dificulta todavía más recoger información sobre violaciones de datos."***[7]

Es decir, aún en un estudio cuyo objetivo era precisamente determinar el estado o la situación del cibercrimen a nivel regional, el mismo reconoce oficialmente la dificultad que se tuvo en el trabajo al intentar recolectar información oficial de los propios organismos públicos y de las grandes empresas, reticentes a colaborar y dar información sobre los incidentes sufridos.

Por otro lado, también es posible citar el *Comprehensive Study on Cybercrime* [8] realizado por Naciones Unidas, en particular por la *United Nations Office on Drugs and Crime* (ONUDC), publicado en Febrero de 2013 y en el cuál se encuestaron a más de 82 países, incluyendo varios de Latinoamérica (entre ellos, Argentina).

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, tanto de los países desarrollados y 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, en nuestro caso, de Argentina.

5. Cifra negra y falta de denuncias

En estrecha relación con el desafío de la falta de estadísticas oficiales, 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 al Dr. Germán Aller [9] 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

---

7 La negrita pertenece a los autores.

que ni siquiera serán atendidas, tratadas ni conocidas por el segmento penal, y a las cuales el Estado no da respuesta alguna. De acuerdo a 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.

De acuerdo a este autor, 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, con el objetivo de 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 demuestra desde hace años los estudios del Índice de Confianza en la Justicia [10] (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.

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). Todos estos aspectos, no suele encontrarse (salvo excepciones) a lo largo de nuestro país, radicando aquí 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, hacen 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, uno de las principales virtudes que analizará un cliente, será precisamente el nivel de profesionalismo en relación 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), las consecuencias hacia su imagen, buen nombre, reputación, etc., puede ser gravemente perjudicada, superando ampliamente el daño ya recibido por el ataque informático en sí mismo.

A modo de mejorar el sentido de este aspecto, se citan dos ejemplos para la facilidad de comprensión de los lectores. Supongamos el caso de una importante empresa dedicada al rubro de la salud (clínica por ejemplo), la cual 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 en base al trabajo de muchos años. Otro ejemplo puede ser el caso de un profesional reconocido en su ambiente (un periodista, un abogado, un psicólogo) el cuál es víctima de un caso de interceptación de comunicaciones electrónicas (cuentas "pinchadas"), permitiendo que terceros extraños accedan a todas sus comunicaciones privadas (y eventualmente difundidas). Fácilmente puede advertirse que los daños ocasionados por una noticia (que vale destacar que son generalmente buscadas atendiendo a la gran recepción que existe en la masa sobre este tipo de casos de problemas "cibernéticos") pueden ocasionar perjuicios irreparables, afectándose 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 por el delincuente informático.

6. Cooperación internacional

Entre los diferentes desafíos inherentes o característicos de los delitos informáticos a nivel mundial, encontramos la posibilidad de que estos puedan ser cometidos sin respetar barreras geográficas o jurisdiccionales. Esto implica que cualquier delincuente informático puede ejecutar acciones desde un determinado lugar, conectándose a sistemas o equipos en otra parte y finalmente atacar datos o sistemas ubicados en otro lugar. La cadena puede tener indeterminadas variables dependiendo de la complejidad del ataque y de los conocimientos del delincuente.

Sin dejar de destacar la importancia que representa, cabe destacar que el elemento de la internacionalidad en los delitos informáticos no es esencial, en consideración que el mismo puede perfeccionarse dentro de la misma red local, en la misma ciudad, Provincia o País. Sin embargo, la inexistencia de barreras geográficas en Internet, permite que los mismos delitos sean realizados desde cualquier lugar del mundo, hacia cualquier otro lugar del mundo.

A los fines de la investigación y persecución de este tipo de delitos, este aspecto puede convertirse en un verdadero obstáculo cuando el delincuente utiliza sus conocimientos para ocultar o simular el verdadero lugar desde donde se realiza el ataque. Esto es posible con una relativa[8] facilidad técnica, donde por ejemplo, un delincuente informático de Argentina, pueda utilizar un servidor *proxy*[9] ubicado en otro país, para atacar un objetivo argentino. A nuestro criterio, esta realidad representa para el Derecho un verdadero desafío a vencer.

En la Resolución AG/RES. 2004 [11] que plantea la Estrategia de Seguridad Cibernética por parte de la Organización de los Estados Americanos (OEA), se reconoce "*La necesidad de crear una red interamericana de alerta y vigilancia para diseminar rápidamente información sobre seguridad cibernética y responder a crisis, incidentes y amenazas a la seguridad de las computadoras y recuperarse de los mismos*". En el citado documento, existe un apartado especial sobre la "*Redacción y promulgación de legislación en materia de delito cibernético y mejoramiento de la cooperación internacional en asuntos relacionados con delitos cibernéticos".*

Las afirmaciones realizadas en este capítulo son contundentes: *"Si no cuentan con leyes y reglamentos adecuados, los Estados Miembros no pueden proteger a sus ciudadanos de los delitos cibernéticos. Además, los Estados Miembros que carecen de leyes y mecanismos de cooperación internacional en materia de delito cibernético corren el riesgo de convertirse en refugios para los delincuentes que cometen estos delitos."*

Estas iniciativas de respaldo a la Estrategia Interamericana Integral de Seguridad Cibernética han sido realizadas en el marco de las recomendaciones formuladas por el Grupo de Expertos [12]. En relación a la internacionalidad de los delitos informáticos, la resolución reconoce que *"La naturaleza sin fronteras de las redes mundiales significa que un único acto delictivo relacionado con una computadora puede afectar o dirigirse a computadoras en varios países".*

Estos casos vuelven a ponen sobre las mesas de los académicos las clásicas preguntas sobre la legislación aplicable, pero sobre todo postula el claro desafío de coordinar distintos ámbitos de colaboración internacional. En relación a este último aspecto, el Convenio de Cibercriminalidad de Budapest [13] 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 posible para su incorporación. En el importante caso de que sea aceptado, nuestro país tiene tareas

---

[8] Considerando que no son necesarios conocimientos avanzados en informática para poder realizarlo.

[9] La palabra en inglés "*proxy*" significa "*intermediario"* en español.

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 poseen la posibilidad de denuncia ante la División de Delitos Tecnológicos de la Policía Federal Argentina o ante el Área Especial de Investigaciones Telemáticos de la Policía Metropolitana, opciones que no existen en la mayoría de las otras Provincias de nuestro país).

7. Desarmonización penal en Latinoamérica

De acuerdo a un estudio de derecho comparado realizado recientemente por el Abog. Marcelo Temperini [14], puede afirmarse 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 sus principales factores, se da el hecho que dichos Estados han optado por diversas posturas político-criminales en relación a sus formas de regular, dando 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 puede observar 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, pueden observarse diferencias en cuanto a los elementos y criterios penales considerados como necesarios para la configuración de un tipo penal en particular.

Esta falta de coordinación u armonización legislativa en la región, permite la existencia de los llamados "paraísos legales", desde los cuáles las bandas organizadas del cibercrimen optan al momento de llevar a cabo determinados delitos informáticos.

8. Centros de Respuestas

A nivel internacional, en materia de seguridad de la información, existen los llamados centros de respuestas (CERT). Sin embargo, es necesario distinguir que no todos están preparados para brindar "respuestas" al ámbito privado (el ciudadano víctima de un delito informático), sino que en su mayoría sólo están preparados para recepcionar incidentes ocurridos en el ámbito público.

En Argentina, dependiente de la Jefatura de Gabinetes de Ministros, se ha creado el ICIC [15] (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.

En países con mayor desarrollo, hace años que existen diversos centros de respuesta para los casos de delincuencia informática. Por citar algunos, se pueden mencionar el IC3 [16] de Estados Unidos, la UNEDEI [17] en México, la CYCO [18] en Suiza. Todos ellos, además de contar con una infraestructura dedicada a la recepción de denuncias por parte de las víctimas, permiten que las propias denuncias puedan ser realizadas de forma electrónica (lo que permite 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 permita la colaboración internacional en casos de cibercrimen.

9. El Proyecto ODILA

El Proyecto ODILA (Observatorio Latinoamericano de Delitos Informáticos) es un proyecto conjunto, llevado adelante por Segu-Info[10] y AsegurarTe[11], a través del Lic. Cristian Borghello (Segu-Info), el Abog. Marcelo Temperini (AsegurarTe) y el A.I.A. Maximiliano Macedo (AsegurarTe). Este proyecto busca construir un espacio de investigación, encuentro y trabajo sobre la realidad latinoamericana en materia de delitos informáticos y cibercrimen, especialmente dedicado a relevar información sobre incidentes o delitos informáticos ocurridos en los países de Latinoamérica.

9.1 Misión

La misión del Proyecto ODILA es brindar un ámbito virtual donde todas aquellas personas que hayan sido víctimas de algún tipo de un delito informático en Latinoamérica, puedan reportar e informar de manera 100% electrónica sobre el hecho ocurrido, a fin de recolectar información que permita saber el estado de situación en materia de delitos informáticos en la región.

9.2 Visión

---

10 Segu-Info: www.segu-info.com.ar

11 AsegurarTe: Consultora en Seguridad de la Información – www.asegurarte.com.ar

El Proyecto ODILA nace a partir de la necesidad de dar a conocer el problema de la cifra negra de los delitos informáticos, informando a la sociedad sobre la legislación vigente y fomentando la necesidad de realizar las denuncias en los casos que ocurran este tipo de incidentes,, convencidos que para poder avanzar en la lucha contra esta problemática, es necesario conocer el estado actual de los datos sobre el estado de situación en los países de nuestra región, algo que en la mayoría de ellos, no existe oficialmente.

9.3 Objetivo General

- Proponer una alternativa que permita combatir el problema de la cifra negra en materia de delitos informáticos en los países de América Latina.
- Generar, sistematizar y difundir información relevante para estudiar, investigar e incidir en la problemática de los delitos informáticos en países de América Latina.

9.4 Objetivos específicos

- Informar sobre el problema de la cifra negra en materia de delitos informáticos.
- Difundir consejos e información útil para las víctimas de delitos informáticos.
- Generar informes y estadísticas propias sobre la ciberdelincuencia en Latinoamérica.
- Fomentar en el usuario la realización de denuncias para los casos de delitos informáticos.

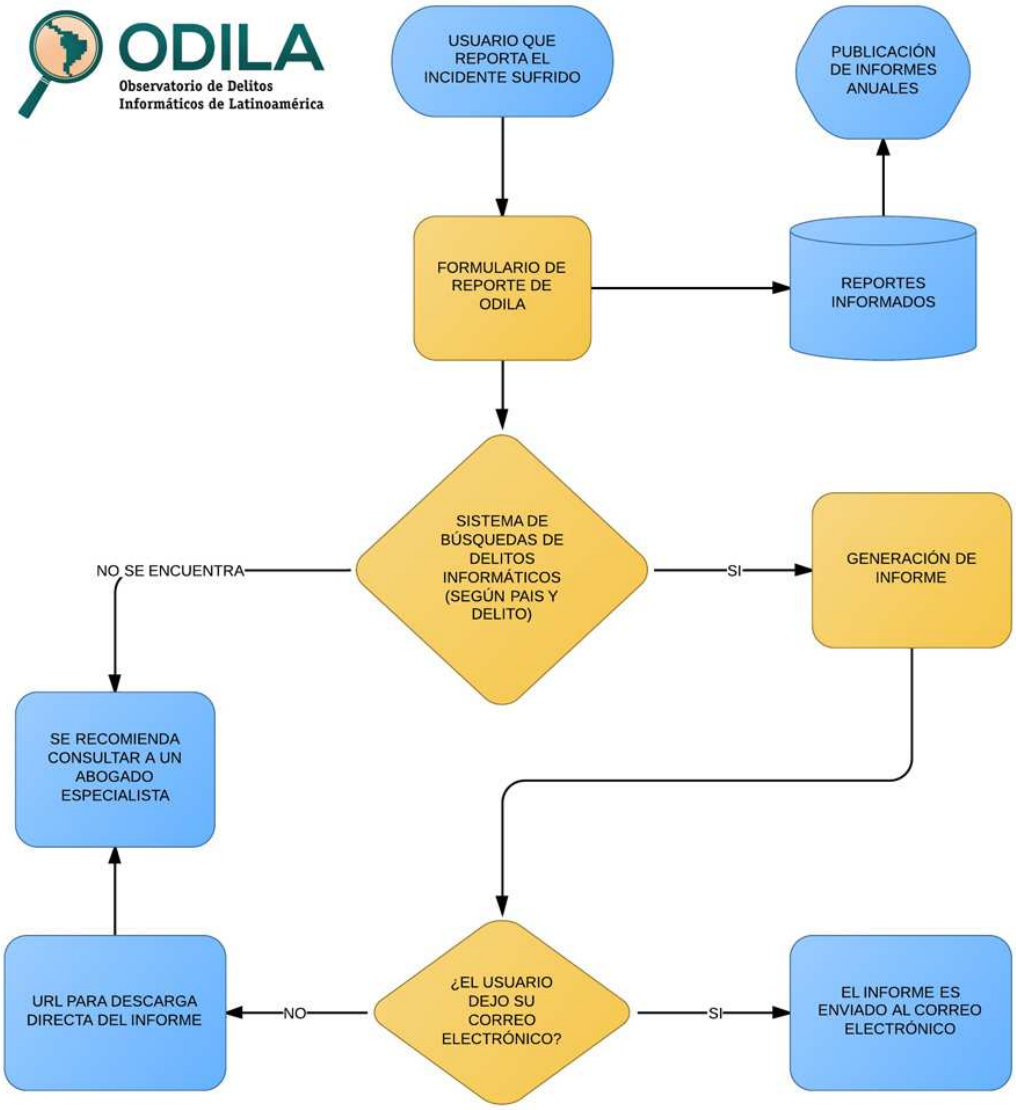
9.5 Metodología y Sistema

El Proyecto ODILA será llevado a cabo a través de su sitio oficial www.odila.org, en el cuál el ciudadano podrá encontrar información sobre el proyecto, legislación sobre delitos informáticos, y sobre todo la posibilidad de reportar el incidente informático que ha sufrido, a fin de poder obtener una guía sobre si el hecho sufrido puede ser considerado un delito informático de acuerdo a la legislación vigente en el país de residencia del usuario.

Como puede observarse en el gráfico de procesos que se acompaña, el sistema se desarrolla a través de distintas etapas:

1) Recolección de información a partir del reporte realizado por el usuario.
2) El formulario es procesado por el sistema, por un lado enviándose a una base de datos de reportes, cuyo objetivo final es la publicación de futuros informes.
3) Por otro lado, parte de esa información (país de residencia y tipo de incidente) es enviada al sistema de búsquedas de delitos informáticos.
4) En el caso que el sistema encuentre que en el país indicado, ese hecho pueda ser encuadrado en algunos de los tipos penales vigentes, el sistema procederá a generar un informe, indicándose dichos artículos así como algunas recomendaciones generales a tener en cuenta y sobre todo, información sobre donde poder realizar una denuncia formal para que se pueda investigar el hecho por parte de las autoridades pertinentes.

5) En el caso que el sistema no encuentre que en ese país, ese hecho pueda encuadrarse en algunos de los tipos penales vigentes, devolverá un mensaje informando sobre tal situación, sumado a la legislación vigente en dicho país (para que el usuario pueda consultarla de forma directa) y sobre todo, una recomendación de consultar y asesorarse con un profesional especializado en la materia.



9.6 Aclaraciones importantes

Es de importancia hacer destacar que el Proyecto ODILA **no pretende ser un asesoramiento para el usuario**, ni mucho menos, razón por la cual se deja en claro que el usuario debe siempre consultar ante un profesional especializado en la materia. Es decir, el sistema no garantiza la exactitud de los resultados en relación a sobre si el hecho efectivamente puede ser considerado un delito penal en el país indicado por el usuario, sino que simplemente brinda un acercamiento a la materia, destacando que su principal objetivo siempre es la concientización acerca de la importancia de dar conocer la problemática, y sobre todo, fomentar la realización de denuncias que permita un combate eficaz frente al problema de la cifra negra.

Por la magnitud del proyecto en cuanto a su intención latinoamericana, así como por las innumerables problemas que pueden presentarse al momento interpretar si un hecho descripto reúne todos los requisitos del tipo penal (algo que podría ser desarrollado por cualquier fiscal o juez), así como las propias complejidades que posee en cada tipo penal en relación a sus requisitos jurídicos, es imposible garantizarle al usuario la exactitud o precisión en los resultados del sistema. Por lo tanto, nuevamente se insiste en que el Proyecto ODILA solamente pretende ser una guía para orientar al usuario (víctima), brindar información sobre la materia y fomentar la realización de denuncias.

En relación a la recolección de datos, se deja aclarado que en dicho proceso no es necesario que el usuario brinde sus datos personales, es decir, que el reporte puede ser realizado de forma anónima. Excepcionalmente, el usuario tiene la posibilidad de informar en el reporte su cuenta de correo electrónico, a fin de que los resultados y consejos puedan ser posteriormente enviados a esa cuenta. Por último, destacar que se ha pretendido que el formulario diseñado, junto con sus preguntas sean lo más sencilla posible, a fin de facilitar su comprensión y por lo tanto su utilización.

Por último, destacar que los datos recolectados, y de acuerdo al caudal de datos que puedan ser incorporados a través del Proyecto ODILA, serán publicados en informes anuales.

10. Conclusiones

El paso de los años demuestra que el problema de los delitos informáticos sigue creciendo y cada vez a pasos más acelerados. Si bien en la mayoría de los países ya se ha dado el primer paso, sancionando penalmente en mayor o menor medida a los delitos informáticos, esto no es suficiente.

A modo general, expresamos una posición que considera necesario el avance sobre reformas y modificaciones sobre la legislación procesal a fin de que se arbitren medios más idóneos para poder perseguir investigar, perseguir y condenar de forma efectiva a los delincuentes informáticos. Una legislación procesal más adecuada y flexible permitirá una mejor recolección de la evidencia digital, elemento vital y necesario para avanzar sobre la problemática.

Es también necesario contar con la colaboración de los ISP, empresas privadas que en la mayoría de los casos de delitos informáticos, son poseedores de información (datos de tráfico) esencial al momento de la presentación judicial de las pruebas de los ilícitos.

En relación a la problemática puntual planteada en el presente trabajo, expresamos nuestra preocupación sobre la falta de estadísticas generales y oficiales sobre delitos informáticos, la cual impide, por ejemplo, determinar qué tipo de delitos son los más cometidos, los bienes jurídicos más afectados, determinar los tipos de objetivos de los delincuentes (empresas financieras, bases de datos personales, etc.), entre otras datos de interés y utilidad al momento de tomar decisiones de política criminal con respecto al problema.

A nuestro entender, la cifra negra existente representa un aspecto sustancialmente problemático que impide desarrollar un trabajo serio de observación, análisis y elaboración de estrategias o planes a mediano o largo plazo orientados a combatir el cibercrimen.

En este marco es presentado el Proyecto ODILA (Observatorio Latinoamericano de Delitos Informáticos), que busca construir un espacio de investigación y trabajo, especialmente dedicado a relevar y recolectar información sobre delitos informáticos ocurridos en Latinoamérica, con la finalidad de generar, sistematizar y difundir información sobre el problema de la cifra negra y la necesidad de fomentar la realización de denuncias por parte de los particulares que sean víctimas.

Es importante expresar que los autores de esta iniciativa, somos conscientes de las limitaciones y errores que pueden darse en el proceso del proyecto planteado, algunas de ellas ya desarrolladas en entre las aclaraciones importantes del proyecto, y otras que seguramente se irán develando a partir de la puesta en marcha del proyecto. No obstante, asumimos el riesgo de equivocarnos y de intentar, aportando una idea y un lugar de trabajo, que a fin de cuentas, más allá de la precisión o calidad de los datos que puedan llegar a obtenerse con el paso del tiempo, siempre tendrá como finalidad última una intención de difusión y capacitación hacia la sociedad sobre la problemática de los delitos informáticos, un flagelo que sigue avanzando y sobre el cual estamos convencidos que debe realizarse un esfuerzo conjunto entre el ámbito público y privado para poder combatirlo.

11. Referencias

[1] SYMANTEC CORPORATION, "2012 Norton Cybercrime Report", septiembre de 2012; http://www.norton.com/2012cybercrimereport Consulta: 15/04/2014

[2] KSHETRI, Nir, "The Global Cybercrime Industry", C Springer-Verlag Berlin Heidelberg 2010, ISBN 978-3-642-11521-9

[3] TÉLLEZ VALDÉS, Julio, "Derecho Informático", 3ª.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8

[4] DAVARA RODRIGUEZ, Miguel Ángel, Manual de Derecho Informático, Thomson Aranzadi, 10º edición, pág. 358 y 359.

[5] FERNANDEZ DELPECH, Horacio, Manual de Derecho Informático, 1ra. Edición, Ed. Abeledo Perrot, Argentina, 2014, Pág. 194

[6] SAENZ, Ricardo. "Informe sobre el relevamiento de causas en la que se investigan delitos informáticos", 2010.

[7] TREND Micro; "Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos", 2013, Secretaría de Seguridad Multidimensional de la OEA. ISBN 978-0-8270-6061-6

[8] NACIONES UNIDAS, New York, 2013. UNODC. Comprehensive Study on Cybercrimen: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf Consultado: 27 de Noviembre de 2013

[9] ALLER, Germán. "Cuestiones Victimológicas de Actualidad: Origen de la Victimología, Seguridad, Cifra Negra, Personalización del Conflicto y Proceso Penal". Revista ILANUD Nro. 27, 2006.

[10] FORO DE ESTUDIOS SOBRE LA ADMINISTRACIÓN DE JUSTICIA, "Indice de Confianza en la Justicia". http://j.mp/1rE9SiB Consultado: 27 de Noviembre de 2013

[11] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, AG/RES. 2004-XXXIV-O/04.

[12] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, Tercera Reunión del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, OEA/Ser.K/XXXIV, CIBER-III/doc.4/03.

[13] COUNCIL OF EUROPE. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF Consultado: 15/03/2014

[14] TEMPERINI, Marcelo; "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte", 1er. Congreso Nacional de Ingeniería Informática / Sistemas de Información. 2013 (CoNAIISI 2013). ISSN 2346-9927

[15] ICIC, "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad": http://www.icic.gob.ar Consultado: 27 de Noviembre de 2013

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

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

[18] CYBERCRIME COORDINATION UNIT SWITZERLAND (CYCO), Suiza. http://j.mp/1lWG9dp Consultado: 27 de Noviembre de 2013