eNAC
e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME

Autor: Jorge A. Obando S. • Consultor en materia de reformas legales y Observatorio de la Justicia y Seguridad de Iberoamérica • COMJIB

Un mejor control del delito informático en Iberoamérica

Introducción y justificación del presente trabajo. En sus distintas manifestaciones por cuanto es un tipo complejo, en la mayoría de las legislaciones de los países iberoamericanos aparece ya tipificado la conducta reprochable relativa al uso de medios informáticos con el objetivo de lograr ventajas ilegales para aquel que cumple con tal conducta. Las reformas legales realizadas han sido de naturaleza especial como los casos de México y Chile o reformas parciales a códigos penales como los casos de Costa Rica y Venezuela. Para efectos de aplicar las políticas de persecución judicial, varios ministerios públicos o fiscales han instalado fiscalías especializadas en este tipo de delito o las han adjuntado a fiscalías ya creadas como puede ser la pornografía infantil en la fiscalía de delitos contra la libertad sexual. Es así que las reacciones para tratar a este tipo de conducta compleja en Iberoamérica han sido diversas. Existen, también, varios grupos de juristas que impulsan acuerdos internacionales regionales con el propósito de lograr instalar normativas mucho más estandarizadas que incrementen la eficacia y efectividad de la política criminal. A pesar de los avances que sin duda existen, consideramos que todavía queda mucho terreno por cubrir en este intento de homogenizar la normativa e incrementar la cooperación, esta última no tanto entre policías sino entre ministerios públicos y judicatura.

A nivel de región y citado estrictamente a título de ejemplo, en el *phishing* (delito relativo a copiar una página web y confundir a la persona que acude a ella, dándole la impresión que está visitando la original) hay una extraordinaria irregularidad normativa y falta de coordinación entre las instituciones. Tiende a perpetrarse este delito cuando se imitan páginas web de bancos o de grandes empresas y se envían correos, de forma masiva, para que los usuarios repitan la entrega de sus datos personales. En Iberoamérica es fácil detectar una ausencia de políticas públicas preventivas de este tipo de delito informático y su impacto está siendo de gravísimo perjuicio para cuentacorrentistas o usuarios de tarjetas de crédito y débito. Aun cuando se conoce acerca de esta modalidad delictiva hace varios años, en la Argentina, por ejemplo, no se le concedió la importancia que tiene sino cuando, en febrero del año 2006, se conoció el primer asunto en que entidades financieras nacionales y sus cuentacorrentistas fueron seriamente afectados. Consistió la actividad ilícita en que a miles de personas se les envió un correo electrónico que les pedía actualizar los datos de sus cuentas bancarias, paradójicamente el mensaje insistía en que la entrega del dato por parte del cliente bancario iba a incrementar la seguridad de sus haberes, los nuevos datos recibidos, ya convertidos en información, se vendieron como listas de correos. En Argentina al no ser considerada la información como un bien, no

JPEN 2008
With financial support from the JPEN Programme European Comission - Directorate - General Justice Freedom and Security

cybex
The Digital Forensic Company

podía ser calificado como delito su robo, modificación o destrucción. En España, como contraste, se considera al plishing como estafa gracias a una interpretación judicial en que se establece que existe una transferencia no consentida llevada a cabo por medios informáticos.

Iberoamérica en la retaguardia normativa. Las incontenibles y aceleradas innovaciones tecnológicas llegan a conformar toda una serie de dificultades que produce la necesidad de tipificar nuevas conductas delictivas. Los estados iberoamericanos, a los inicios de los noventa, quedaron obligados a generar descripciones de conductas y a acordar normativa que las regulara, sin embargo la reacción ha tomado mucho más tiempo que el esperado, posiblemente por las dificultades teóricas de la definición y por la lentitud de los sistemas legislativos para ajustarse a los problemas coyunturales. Todavía a finales de los años noventa (1999), autores como Julio Nuñez Ponce escribían que "es necesario fortalecer la conciencia jurídica iberoamericana de que este tipo de delitos (informáticos) es beneficioso que tenga una represión penal que tenga elementos comunes entre los diversos países, de forma tal que pueda haber una sanción eficaz aún cuando se cometan simultáneamente por medios telemáticos en distintos Estados." Repetimos que se ha avanzado mucho en los últimos diez años, sin embargo todavía no se ha logrado la tan ansiada coordinación institucional ni la uniformidad normativa, e incluso existen desconfianza entre los países en el sentido que algunos de ellos puedan compartir la inteligencia existente con los grupos criminales.

En general se considera delito informático aquellas conductas ilícitas susceptibles de ser perseguidas efectivamente, en sede judicial, con base en tipos previamente definidos por la normativa penal, general o especial, que hacen uso inadecuado de cualquier medio informático. Repetimos que es un delito complejo, el cual en un primer momento los países iberoamericanos intentaron ajustar a figuras penales conocidas como el robo, hurto, fraude, estafa.

Otro autor, Tellez Valdés, estableció a finales de la década de los noventa una doble clasificación de este tipo de delitos, utilizando los conceptos de medio y objetivo. La primera clasificación, la de medio, incluye la falsificación de documentos (cheques o talones bancarios), variación de los activos y pasivos en los balances contables de las empresas, simulación de delitos convencionales como el fraude, robo de tiempo de trabajo de expertos, sustracción de información clasificada, modificación de datos, el denominado "caballo de Troya" que consiste en penetrar un sistema introduciendo instrucciones no coincidentes con los intereses de los propietarios o usuarios de tal sistema, variación manipulada del destino de pequeñas cantidades de dinero en gran número de cuentas corrientes bancarias o cuentas de tarjetas de crédito y alteración en el funcionamiento de los sistemas mediante la introducción de virus informáticos. La

segunda clasificación, la de objetivo incluye especialmente a la pornografía y aparecen también , como ejemplos, el secuestro de soportes magnéticos para efectos de extorsión y el sabotaje político en que hay un apoderamiento de los sistemas de inteligencia o de policía de un país.

El Código Penal Peruano, como ilustración de tipificaciones nacionales, incluye dentro de los delitos informáticos al delito de violación a la intimidad, el delito de hurto agravado por transferencia electrónica de fondos, el delito de falsificación de documentos informáticos, el delito de fraude en la administración de personas jurídicas y los delitos contra los derechos de autor de software. Es así que el Código Penal Peruano establece que "el que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres y treinta a ciento veinte días cuando el agente revela la intimidad conocida de la manera antes prevista"; también establece este código que "el que indebidamente organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años. Si el agente es funcionario o servidor público y comete delito en el ejercicio del cargo, la pena será no menor de tres años ni mayor de seis e inhabilitación". Otro ejemplo del tipo de tipificación incipiente que un código iberoamericano contiene se refiere a lo dicho por el Código Peruano en el sentido que "…para obtener provecho, (el actor) se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equipara a bien mueble la energía eléctrica, el gas, el agua y cualquier otro elemento que tenga valor económico, así como el espectro electromagnético". Finalmente y para ilustrar el delito de falsificación de documento informáticos, en legislación especial peruana se establece que "la falsificación y adulteración de microformas, microduplicados y microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme a las normas pertinentes del Código Penal".

En otro país iberoamericano, Uruguay, se propuso a finales de la década de los noventa la tipificación del delito informático y por separado del delito de hurto informático. Es así que la reforma legal establece que "el que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial, indebido, o causare un patrimonio de otro, operando un proceso de datos incorrecto, configurando incorrectamente un programa de software, empleando adrede datos falsos, incorrectos o incompletos, o a través de cualquier otra intervención o manipulación ilegítima, sin la debida autorización o excediéndose de la misma, será castigado con pena de dos a seis años de penitenciaría". Vemos, entonces,

las diferentes aproximaciones y tratamientos que se le han venido dando al delito informático.

En consecuencia lo que se confirma en este *non paper* es que el proceso de legislación y de persecución iberoamericano, relativo al delito informático, ha sido muy irregular y desfasado en relación con lo que en otras regiones del mundo se ha hecho. Es por esto que Alfredo Sànchez Franco afirma en un artículo titulado Delitos Informáticos y su Prueba (algunas consideraciones sobre la ley penal mexicana, con base en la legislación penal internacional) que "En la información contenida en estas páginas, se refleja el atraso de la ley penal mexicana (en la parte especial y en lo procesal) en relación al vertiginoso avance que cada año --en ocasiones en menos tiempo—caracteriza a la denominada INTERNET (International Network) y a las diversas herramientas virtuales que son creadas para vestir y actualizar cada año a dicha invención, que se ponen a disposición y servicio, gratuito u oneroso, de millones de usuarios a nivel mundial y por consecuencia, desafortunadamente se constata dicho atraso, si se le compara, inevitablemente, con las leyes penales que se están implementando a nivel internacional para describir y combatir los llamados cyberdelitos o delitos informáticos".

Conceptos relevantes. Stephanie Perrin nos ayuda a aclarar, en un artículo escrito por esta especialista canadiense en el 2006, el concepto de delito informático. El término se logró acuñar a finales de los años noventa a medida que crecía la Internet. Al fundarse el ya bien conocido G-8 (actualmente sustituido por el G-20), se utilizó el término de manera muy imprecisa, para describir los tipos de delitos perpetrados mediante utilización de Internet o de las nuevas redes de telecomunicaciones.

El Consejo Europeo inició actividades dirigidas a diseñar el Tratado sobre el Delito Informático y el mismo no fue presentado a la opinión pública no antes del año 2000. En este tratado existe una muy interesante recopilación de políticas públicas que, aun cuando algunas de ellas ya han sido adoptadas en América Latina, representan un catálogo innovador de estrategias. El Tratado no define el concepto de delito informático lo cual responde a las tendencias normativas y de políticas públicas de vanguardia. El Tratado sugiere de la siguiente forma y manera las áreas temáticas en las cuales se requiere generar nueva normativa y establecer sólidas políticas criminales de Estado y políticas de persecución judicial:

> En su título primero aparecen los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. En el segundo aparecen los delitos relacionados con las computadoras de falsificación y fraude. El título tercero se refiere a delitos relacionados con el contenido, específicamente la pornografía y dentro de ella la pornografía infantil. El título cuarto se refiere a delitos relacionados con la violación del derecho de autor y los derechos

asociados. Finalmente el título quinto abarca las responsabilidades secundarias y sanciones, lo que incluye a la cooperación delictiva y la responsabilidad empresarial.

Lo claramente destacable del Tratado es que se refiere a reformas de carácter procesal y a la cooperación internacional. Estas áreas son precisamente, repetimos, en las que se pueden percibir los espacios para crecer más sensibles en Iberoamérica. Está claro que siendo el derecho penal efectivo siempre y cuando exista clara evidencia, en relación con delitos informáticos los procesos judiciales exigen nuevas técnicas para recoger y utilizar la prueba, asegurar su integridad y coordinar su utilización a nivel internacional.
Se quedó corto el Tratado en el sentido de la tutela del derecho fundamental de privacidad y protección de los Derechos Humanos. El Tratado confirma que al no tener Internet fronteras, la persecución judicial debe adoptar esta característica. Es así que la cooperación internacional es esencial a la efectiva prevención, represión e investigación del delito informático. Así mismo otra característica de énfasis del Tratado se refiere a la inclusión de normas en la legislación relativas a la "piratería informática", ello por cuanto en muchos países no existe efectiva normativa, y menos políticas, que permitan el control de este tipo de actividad delictiva que tanto ha distorsionado a los mercados.

El Tratado también toca un tema de gran trascendencia y son los juegos al azar en línea. Al surgir desde pistas de carreras virtuales como loterías o casinos y a pesar que varios países ya habían variado, con base en la experiencia interna, su criterio acerca de la posibilidad de gravar con tributos posibles a los juegos de azar, se requería una actitud no ingenua para el control de tales juegos. El Tratado dialoga claramente con la ambición fiscal y lo lleva a considerar que las ganancias en los juegos de azar por Internet son de muy difícil control fiscal.

¿Es el delito informático un delito virtual?. El concepto de ciberespacio, acuñado por William Gibson en los inicios de los años ochenta, en realidad carece de contenido material y por lo tanto es válido decir que no existe. Lo que existe es la red de Internet, los que existen son los servidores y los equipos de cómputo. El delito, para serlo desde la perspectiva legal y judicial, necesariamente debe producirse en el mundo real que se percibe mediante los sentidos. En un inicio se dieron discusiones bizantinas acerca de si el hecho que un hacker "mirara" fisuras en la seguridad ya se consideraba un delito. Este tipo de juego intelectual en relación al delito informático exige una tipificación cerrada y de alta precisión que no permita mayor espacio para interpretaciones judiciales de carácter seudo-garantista que genere un mundo de impunidad alrededor del delito informático. La investigación o logro de evidencias de un delito que no se materializa como los demás delitos, obliga a regular el mecanismos de confiscación de hardware.

Tanto la institucionalidad como las normas requieren una muy especial lectura acerca de que el concepto de delito informático puede ser incluso innecesario por cuanto podría conducir a un destaque excesivo de su intangibilidad. Aun cuando los medios son determinantes del tipo penal, el resultado es lo conclusivo para incluir a este tipo de conducta dentro del menú de las perseguibles por el Derecho Penal.

Conclusiones.- Tres principales conclusiones para el mundo institucional iberoamericano, en relación al así llamado delito informático, se logran del presente trabajo:

A.- Los países iberoamericanos requieren todavía una importante cantidad de trabajo en materia de reforma normativa, pero donde se debe concentrar la actividad es en la reforma procesal y en la coordinación internacional e inter-institucional.

B.- Una muy buena guía de trabajo para los países iberoamericanos lo constituye el Tratado Europeo sobre el Delito Informático del 2001. La accesibilidad de este texto y de la doctrina jurídica que ha generado, es clave para crear una nueva conciencia en los gobiernos y las sociedades civiles iberoamericanas.

C.- Hay que apartarse de las definiciones, particularmente al momento de formular reformas normativas, por cuanto el delito informático carece de la tangibilidad propia de otros tipos de figuras penales.

Autores citados: **Julio César Nuñez Ponce**. Especialista peruano y autor de "Software:Licencia de Uso, Derecho y Empresa". Fondo de Desarrollo Editorial de la Universidad de Lima, Perú, 1998.

Julio Tellez Valdez.- Investigador titular "B" de tiempo completo en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, en Derecho de la Información. (líneas de investigación: Derecho de las Telecomunicaciones, Derecho e Informatica e Informática Jurídica. Autor de "Derecho Informático", editorial McGraw-Hill, 1998.

Alfredo Sánchez Franco- Especialista mexicano y abogado practicante del Derecho Informático en la Ciudad de México. Autor de "Delitos Informáticos y su Prueba" de México. Ensayo No. 1 sobre el tema de investigación de delitos informáticos, en el Master en "Derecho Penal, Constitución y Derechos" por la Universidad Autónoma de Barcelona, España (U.A.B.). 2002-2003.

Stephanie Perrin. Consultora especializada en materia de vida privada y de política de información. Consejera industrial para el Estado y la sociedad civil sobre la puesta en marcha de procedimientos y de políticas de protección de datos y sobre el impacto de las nuevas tecnologías en la vida privada.Es Coordinadora de la Investigación para el proyecto *Anonymity* (Anonimato), radicada en la Universidad de Ottawa. Es miembro ejecutiva del *Centro de Información sobre la Privacidad Electrónica* (EPIC) en Washington y trabaja con otras organizaciones de defensa en Canadá e internacionalmente. Stephanie contribuyó positivamente en la elaboración de las políticas de privacidad y criptografía de Canadá durante quince años.

William Ford Gibson. Nacido en 1948, es un escritor estadounidense-canadiense a quien se le ha llamado el "profeta negro" debido a su obra de ciencia ficción acerca del espacio cibernético. Específicamente Gibson acuñó el concepto de Ciberespacio en su obra "Burning Chrome" y luego popularizó el concepto en su novela *Neuromancer* (1984).

JPEN 2008
With financial support from the JPEN Programme
European Comission - Directorate - General
Justice Freedom and Security