Artículo de actualidad

El hacker y sus conductas
The hacker and its behaviors
Hacker kuéra ha hekovekatu

Giovanni Michelle Grisetti Valiente[*]

Ministerio Público de la República del Paraguay

Recibido: 30.11.16 Aceptado: 09.12.16

Resumen

El avance tecnológico en la actualidad es incesante y con esta realidad surgen nuevas formas delictivas. Una de esas modalidades es el acceso no autorizado a redes informáticas. Esta particularidad tiene vertientes y una de ellas es el hacker, que a su vez se conocen dos comportamientos diferentes, una de ellas la del hacking ético y cuando actúa de una manera ilegal se denomina cracker. La primera figura es la que se analizará en esta oportunidad y representa a la persona que ingresa sin autorización a una red informática con el solo fin de observar, advertir errores, falencias y hasta recabar datos sobre hechos punibles del usuario hackeado. Por ello, el Derecho Penal a nivel internacional ha reprimido este tipo de conductas, por lo que se sugiere tomar esa tendencia para la legislación nacional. Con ese fin, se realiza una descripción de los prototipos penales que castigan

*** AgenteFiscal, Director de Denuncias Penales del Ministerio Publico, Asunción, Paraguay. Email: giogrisetti@gmail.com.**

Egresado de la Universidad Nacional de Asunción, año 2009. Notario y Escribano Publico, egresado de la Universidad Privada del Este. Diplomado en Dogmática Penal en el Centro de Ciencias Penales y Política Criminal. Diplomado en Derecho Penal Económico. Diplomado en Derecho Constitucional de la Universidad di Bologna (Italia). Especialista en Ciencias Penales por el Centro de Ciencias Penales y Política Criminal. . Docente e Investigador del Centro de Entrenamiento, funcionario de carrera fiscal, desde el año 2003, como practicante, notificador fiscal, secretario fiscal, asistente fiscal y relator fiscal. Cargo Actual, Agente Fiscal, Director de Denuncias Penales del Ministerio Publico, Paraguay, Asunción.

estas conductas y se señalan las fortalezas y debilidades del tipo penal que rige el en país. Además, se identifica el bien jurídico protegido, que tiene amplia relación con el Derecho a la Intimidad resguardado constitucionalmente y más específicamente puede denominarse Derecho a la Intimidad Informática, que precisa una regulación especial al considerarse delictiva y posterior a la vigencia de la Constitucional Nacional y la legislación penal vigente. La investigación tiene un enfoque descriptivo, de carácter cualitativo pues mide la calidad de la respuesta penal a los actos delincuenciales contemporáneos.

Abstrac

The technological advance at present is incessant and with this reality arise new criminal forms. One such mode is unauthorized access to computer networks. This particularity has slopes and one of them is the hacker, which in turn are known two different behaviors, one of them the ethical hacking. This figure represents the person who enters unauthorized into a computer network for the sole purpose of observing, warning errors, shortcomings and even collects data on punishable acts of the hacked user. For this reason, international criminal law has repressed this type of conduct, so it is suggested to take that trend for national legislation. To that end, a description is made of the criminal types that punish this type of behavior and indicate the strengths and weaknesses of the criminal type that governs the country. In addition, it identifies the protected legal property, which has broad relation with the Right to Privacy protected constitutionally and more specifically can be called the Right to Information Intimacy, which requires special regulation when considering criminal conduct after the validity of the National Constitutional and The current criminal legislation. The type of

investigation is descriptive, of qualitative character since it measures the quality of the criminal response to the contemporary delinquency acts.

Ñembyapu'a

Ko'ã tecnología ojeporu poruve ko'ãga rupi ha upéicha rupi osẽ osẽve opaichagua tembiapo vai apo, jaikuaami peteĩ tembiapo vai, péicha ojeikérõ mbaretépe umi ñanduti ryepýpe, redes informáticas rupi. Ko'ãva ojejuhu heta hendáicha ojejapo, peteĩva héra hacker, kóva avei oĩ 2 hendáicha, peteĩ héra hacking ético. Koichagua pe tapicha oikéva kañyhápe, mavave ojerure'ỹre ichupe peteĩ red informática ryepýpe, ha'e oike ojesareko haguã, omyatyrõ ojejavývape ha ombyatypa kuaa opa mba'e oĩva upépe, upe ojeahckeáva mba'épe. Upévare, pe Derecho Penal Internacional ojopy ha ojoko voi kóichagua tembiapo vai ha ojehecha porã tekotevẽha oñemoinge avei ñande léipe. Upevarã ningo oñemyesakã hína mba'eichagua léipa ikatu ocastiga kóichagua tembiapo vai, ha ojehechauka avei mamópa imbarete ha mamópa ikangy hína ñande léi kuéra upevarã. Upéicha avei ojejuhu ojeheróva bien jurídico protegido ha péva ojogueraha mbarete ambue yvypóra mba'e teére hérava Derecho a la Intimidad Informática, oikotevẽva avei peteĩ léi heseguaitéva ojejuhu rupi ko tembiapo vai ojekuaaha ñande Léi Guasu ha legislación penal jarekóva rire. Ko investigación ohesa'ỹijo ha omombe'u mba'éichapa, oñamindu'u paite opaichagua tembiapo vai osẽva ko'ãga rupi.

Palabras clave: Redes informáticas, hacker ético, vulneración, sanción, ciberseguridad.

Keywords: Computer networks, ethical hacker, infringement, sanction, cyber security

Ñe'ẽ tee: Ñanduti guasu informática rehgua, hacker hekokatúva, jejopyreíva, jejopy, ciberseguridad.

Problemática actual

Al momento de tratarse la reforma penal a la ley de Teodosio González, una de las novedades a incorporar a la reforma, fue la de considerar la protección a las nuevas formas de ataque que comenzaron a padecer las personas en su intimidad, honor, la información privada, entre otros.

En ese sentido, el Prof. Schöne, uno de los proyectistas de dicha reforma penal, señaló como punto de partida para el actual Código Penal:

> Hoy en día la delincuencia no, es más, para decirlo así "interpersonal" como el homicidio, la Lesión, el hurto o la estafa, sino afecta pluralidades de personas indefinidas como por ejemplo en el campo ecológico o económico y también perjudica nuevos bienes como en el área de la informática. (2008, pág. 2).

Luego de entrada en vigencia la Ley n.° 1160/97: "Código Penal Paraguayo", se incorporaron tipos penales en atención al avance de las tecnologías con el acompañamiento de las eventuales conductas que pudieran cometerse a través de ellas.

Posteriormente se introdujeron nuevas modificaciones a la referida ley de fondo en adecuación a las recomendaciones de la Convención sobre la Ciberdelincuencia, celebrada en Budapest en el mes de noviembre de 2001, y en parte al Derecho Penal Alemán que contempla la protección de bienes jurídicos que pudieran ser lesionados a partir de conductas que surgen con el avance de la

tecnología.

En ese sentido, la Ley n.° 4439/2016 "delitos informáticos", incorpora nuevos tipos penales al catálogo de hechos punibles previstos en el Código Penal Paraguayo, que guardan relación con la ciberdelincuencia, tipificando los expresamente los Delitos Informáticos.

Dichos artículos son: 146b "Acceso Indebido a Datos, 146c "Interceptación de Datos", 146d "Preparación de Acceso Indebido e Interceptación de Datos", 174b "Acceso Indebido a Sistemas Informáticos", 175b "Instancia" (del art. 174 y art. 175), y 248b "Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago".

Cabe mencionar que de los citados hechos punibles algunos se castigan desde su fase de actos preparatorios, de esta forma el legislador estipuló por el grado de peligrosidad que representa para un estado que una persona posea un software o hardware con fines ilícitos.

En otros términos, que con dichas herramientas físicas o de programación, se accedan a claves de acceso u otros códigos de seguridad de terceros, que permitan el obtener datos que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible. Algunas formas modernas de actos preparatorios, por citar algunos de ellos son los casos de keyloggers (hardware o software que registra las teclas presionadas); o, phishing (técnica utilizada para obtener ilícitamente datos personales).

En este punto, es preciso ahondar un poco acerca de los keyloggers, denominación dada al hardware o software con la función de grabar cada presión

de teclas que se haya realizado al escribir en un teclado, es decir, puede registrar todo lo que se teclea en cualquier sistema informático. Y se puede almacenar la información en un archivo o transmitir por la red internet a algún email.

Estos programas pueden ser instalados teniendo o no acceso a la computadora de la víctima. Puede instalarse de forma remota y acceder a las contraseñas, a nuestras direcciones de correos, datos bancarios, financieros, o incluso al extremo de controlar las informaciones que la pareja pudiera haber escrito a través de un teclado que tenga un keylogger oculto y utilizar la computadora sin que la persona se diera cuenta. A algunos antivirus pueden detectar este tipo de software, conocidos también como malware (software malicioso).

Así como del phishing, éste último tuvo mucha repercusión con un hecho ocurrido contra el Banco Itaú, específicamente se creó una página web para obtener ilícitamente datos, una página web distinta al www.itau.com.py (dirección web oficial), en otras palabras se emuló a la web del Banco Itaú (Abc Color, 2016) y con esta página web falsa, semejante a la utilizada por el referido ente bancario.

Primeramente, los hackers procedían a enviar emails a través de los cuales solicitaban a los clientes del ente, la actualización de datos personales incluidos las contraseñas o passwords.

De esta manera se obtenían los datos personales, bancarios y lo más importante las claves de las personas que erróneamente creían cumplir con los requisitos del banco.

Una vez que los hackers consideraban que todos los datos ya colectados

en su "trampa", procedían a usar las informaciones de las víctimas quienes confundidos por la −campaña de actualización de datos personal− fueron perjudicados patrimonialmente.

Por casos como los señalados anteriormente es que el Estado debe prohibir determinados actos incluso en su etapa de preparación de modo castigar este tipo de conductas antes de que el resultado sea consumado.

Pocos son los casos de sanción de actos preparatorios en nuestro ordenamiento jurídico penal, los delitos informáticos no son los únicos que poseen esa "consideración". También existen otras puniciones por actos preparatorios en nuestro código penal como ser los tipos penales descritos en los arts. 266 "Preparación para la producción de moneda y marcas de valor no auténticas", art. 270 −Preparación de un atentado contra la existencia del Estado− y 271 del C.Pág. Preparación de una Guerra de agresión.

En esta ocasión se analizará al art. 146b "Acceso Indebido a Datos" y la nueva tendencia del hacking ético a nivel mundial, o también conocidos como hackers buenos o hackers malos.

Marco jurídico

El art. 1° de la Ley n.° 4439/2011, que amplía el art. 146 del Código Penal Paraguayo (Ley n.° 1167/97), y por el cual queda como sigue: art. 146b – Acceso indebido a datos, que reza:

> 1°. El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena

privativa de libertad de hasta tres años o multa.

Al iniciar el análisis se desprende que la norma prohíbe obtener datos protegidos contra acceso no autorizado, sin consentimiento y violando los sistemas de seguridad.

Al ser un tipo penal novedoso, que ha surgido de la evolución de la informática y su influencia en la sociedad actual, determinar el bien jurídico protegido es aún confuso.

Como delito de mera actividad, en la que el resultado del acto es irrelevante para su penalización, se debe individualizar cual es el ámbito de protección de la norma. Aquí nos encontramos con que el Derecho a la Intimidad, tanto de personas físicas como personas jurídicas, se desprende como un derecho inalienable a proteger.

De hecho, el Derecho a la Intimidad se encuentra protegido en su generalidad en nuestra Constitución Nacional en su art. 33.

> **Artículo 33 C.N. - Del Derecho a la Intimidad**
>
> La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte el orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública.
>
> Se garantiza el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

Sin embargo, esta interpretación textual, aun no satisface las necesidades

del tipo penal, principalmente porque la redacción corresponde a una época anterior al avance informático a gran escala. El artículo en cuestión, en su espíritu, va direccionado a la protección de la intimidad del domicilio, así como de los actos de la vida privada, apuntando más bien a la esfera familiar.

Por ello, un acceso indebido a datos, sin haber causado daño alguno se confunde en la legislación. Muy acertadamente Salvadori señala el reciente surgimiento de un nuevo interés jurídico a proteger que es la intimidad informática y agrega que "lo que debe protegerse es la mayor utilidad que consigue el usuario a través de una utilización y goce exclusivo de estos espacios virtuales y que permiten un libre desarrollo y una libre exteriorización de la persona humana". (Salvadori, 2013, pág. 119).

Así el acceso abusivo de sistemas informáticos, el mero intrusismo, tendría un solo requisito para poder circunscribirse como injusto penal. El sistema informático vulnerado, deberá tener al menos una medida de seguridad, sin importar su grado de complejidad. Con este quebrantamiento, la conducta se subsume al tipo penal independientemente al resultado, pues no posee la autorización de ingreso del titular.

Aquí se desprende que este tipo penal se halla −clasificado− como delito de puesta en peligro. La problemática surge a partir de la nueva actividad en auge, a nivel mundial, conocida como el ethical hacking o hacking ético, se dio inicio a una discusión por parte de los juristas y los informáticos, acerca de la no sanción en casos donde el hacking realizado no sea ejecutado con el fin de perjudicar y en ese caso si ¿sería punible o no?

Por ejemplo, si una persona (autor) ingresar a una cuenta digital del banco, debido a que logró descifrar la contraseña de acceso, sería una conducta que podría subsumirse ya en el art. 146b, inc. 1°, primera alternativa. Ahora bien, en caso que el autor, luego del acceso indebido a la cuenta, realice una operación que menoscabe el patrimonio, ya entrará en consideración el art. 188, inc. 1° del C.Pág., núm. 3; o si luego cambiara la contraseña, impidiendo el acceso a dicha cuenta digital bancaria, lo que a su vez violaría el art. 174, inc. 1°, numeral 4.

De la descripción realizada se desprende que con una misma acción natural se violan/violó varias disposiciones penales, lo que arrojaría la aplicación del concurso de hechos punibles, conforme lo establece el art. 70 del C.P.

En cuanto al tipo subjetivo del acceso indebido a datos previsto en el art. 146b, se debe apuntar que solo se castiga la conducta dolosa, basta el dolo eventual. El marco penal es de hasta tres años de pena privativa de libertad o multa.

Análisis del acceso indebido a sistemas informáticos

La ubicación sistemática del art. 174b acceso indebido a sistemas informáticos, resulta incongruente con las conductas castigadas, pues estas parecen estar protegiendo el derecho a la intimidad. Es más, lo que se pretende castigar ya está amparado por el art. 146b, Acceso indebido a datos. Asimismo, el art. 174b, introduce el elemento −sistemas informáticos− lo que dentro de Código Penal se torna confuso.

Según la definición dada por el citado artículo, una computadora podría considerarse un sistema informático. Si a esto se suma que una de las conductas es acceder al sistema informático utilizando la propia identidad, entonces, cual-

quiera que use un ordenador estaría realizando una violación a la norma establecida en el art. 174b –primera alternativa– cuestión merecedora de un estudio modificatorio por parte del Congreso Nacional.

Tomando como base una casuística relacionada al 174b –primera alternativa– si una persona accede a un sistema informático sin autorización y accede a una aplicación o software de un ente bancario, sería una conducta que podría subsumirse en el art. 174b inc 1°, segunda alternativa e igualmente una conducta establecida en el art. 146b, inc. 1°, primera alternativa.

Ahora bien, en caso que el autor, luego del acceso indebido a la cuenta bancaria, realice una operación que menoscabe el patrimonio ajeno, ya entraría en consideración el art. 188, inc. 1° del C.P., núm. 3; o eventualmente, si luego cambiara la contraseña, impidiendo el acceso al titular a la misma cuenta bancaria, también se violaría el art. 174, inc. 1°, cuarta alternativa. Rápidamente, del caso se desprende que con una misma acción natural se violó varias disposiciones penales, quedando habilitado el estudio para la aplicación del concurso de hechos punibles, conforme las reglas establecidas en el art. 70, inc. 1° del C.P., de la Medición de la pena en caso de varias lesiones:

> Cuando el mismo hecho punible transgreda varias disposiciones penales o la misma disposición penal varias veces o cuando varios hechos punibles del mismo autor sean objeto de un procedimiento, el autor será condenado a una sola pena que será fijada en base a la disposición que prevea el marco penal más grave. Dicha pena no podrá ser inferior a la mínima prevista por los marcos penales de las otras disposiciones lesionadas.

2º La pena podrá ser aumentada racionalmente, pudiendo alcanzar la mitad del límite legal máximo indicado en el inciso anterior. El aumento sobrepasará el límite legal máximo previsto en éste código para la pena privativa de libertad y la multa.

3º Cuando una de las disposiciones lesionadas prevea, obligatoria o facultativamente, una prohibición de conducir o una medida, el tribunal deberá ordenarla junto con la pena principal.

Del caso también queda la pregunta si vale ya castigar al acceder a un sistema informático o al acceder a datos

Identificación de la problemática y posibles salidas

En estos tiempos modernos en que la tecnología avanza a pasos agigantados se nos provee de nuevas facilidades en diferentes ámbitos, pero así también esto crea nuevos inconvenientes del cual el Derecho no se sustrae, pues la tecnología mal utilizada es una fuente de nueva criminalidad de diversas formas (citas las formas, tráfico de menores, phishing, etc)

La conducta inicia con una persona a quién se lo conoce virtualmente como hacker, el camino que prepara y sigue para lograr su fin mediante el uso de un sistema informático, a partir de ahí su relevancia en los hechos punibles Informáticos.

Según el diccionario de la Lengua Española, "*hacker* es un pirata informático: Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta" (Diccionario de la Lengua Española, 2016).

Los *hackers* impactan en el mundo real a través de la informática, es decir, un mundo virtual, ¿cómo repercuten sus conductas en el mundo real? Al ocurrir un hecho, surge todo un nuevo paradigma, teniendo en cuenta que un hecho es todo acontecimiento en el mundo real susceptible de ser comprobado y, sin embargo, en concreto la conducta del hacker se realiza en un mundo virtual y de ahí a lo real.

En ese sentido, se afirma que hay un hecho en atención a que las conductas desplegadas en el mundo virtual son comprobables y más aún si impactan en el mundo real. Algunos ataques realizados por *hackers* a los sistemas informáticos como fueron casos de las páginas web de instituciones gubernamentales, fueron con la finalidad de alterar o apropiarse de información de terceros para:

1) su posterior difusión;

2) para hacer reivindicaciones sociales; o,

3) como parte de la ciberguerra que se libra en internet entre potencias rivales.

El Paraguay no queda atrás, en los últimos años ha ganado territorio la influencia de los *hackers*, y en general, está relacionado a obtener información, con ánimo de lucro.

Así mismo, la Agencia de Información Pública del Paraguay (Portal Oficial del Gobierno) fue *Hackeado*, en más de una ocasión fue blanco por motivos políticos, así como el ataque que sufrió la cuenta del twitter del Ministerio del Interior y de la Secretaria de la Información, SICOM, el 23 de julio del 2015,

oportunidad en que se refirieron negativamente en contra del Presidente de la República del Paraguay.

Además, el hecho de que la mencionada institución, encargada de las políticas de seguridad interna, había sido atacada y posterior a ello, fue celebrado por el hacker como una victoria por tal logro en el mundo digital, proveniente de una persona física hacia un estado "virtual". Esta modalidad ha generado un cambio en los antiguos rituales de reclamos que mediante manifestaciones o marchas buscaban causar consecuencias políticas.

Violación de la Información en el sector privado.

El sector privado también es objeto de los accesos indebidos, y hace tiempo que está en la mira de los hackers, cuyo objetivo es beneficio patrimonial indebidamente, datos no autorizados, información confidencial, secretos empresariales, derechos de autor, etc. de las empresas, mediante la interceptación de correos electrónicos y telecomunicaciones, inutilización de sistemas de protección contra virus, *phising, pharming, spam* y otros.

Funcionalidad de los *Hackers* éticos.

No todos los *hackers* se dedican a cometer hechos punibles. Y debido a que los servicios de seguridad de las empresas (en especial, bancos, financieras, etc) muchas veces se ven frágiles ante ataques de esta naturaleza, entonces contratan a hackers y así tratar de paliar los efectos de estos ciberataques para que hagan el llamado *hacking* "ético", o como acostumbran llamar, auditorías informáticas. De este modo queda nuevamente la manera en que se consiente todo posible acceso indebido a sistemas informáticos.

Las Instituciones Públicas de la región, están empezando a ver las ventajas de este sistema y, en esta línea, con la finalidad de poner a prueba su seguridad cibernética e identificar posibles brechas de seguridad en sus plataformas tecnológicas.

El hacker ético implementa algunas medidas de ciberseguridad que son:

1) monitorización, que es un producto que incluye la de vigilancia de sistemas y páginas web, en principio pasiva, sin perjuicio de que se suele acompañar de paquetes de medidas de defensa; y,

2) "*hacking* ético", actividad que trata de adelantarse a la vulnerabilidad mediante pruebas para burlar la seguridad de la red para sustraer información privada y de esta manera encontrar vulnerabilidades, sin generar daños, para que luego se puedan diseñar medidas de protección eficaz.

Estas −ciberpruebas− se instrumentalizan a través de auditorías que pueden realizarse en coordinación con los responsables informáticos de la organización, de forma que éstos sean conscientes en todo momento del grado de intrusión que están sufriendo sus sistemas, hasta el punto de que indican a los auditores (hackers) las posibles debilidades para que sean chequeadas por éstos.

Enfoque jurídico

Desde el punto de vista legal, la cuestión que puede plantearse es si en el desarrollo de estas actividades podrían cometerse algún ingreso indebido a sistemas informáticos regulados en los artículos 174b del Código Penal, ya que los hackers que realizan estos ataques −pactados− cumplen con el fin y acceden a los sistemas informáticos, recabando datos e información como prueba de éxito.

La respuesta debe ser negativa, pues quedaría excluida ya la tipicidad

ante la existencia del consentimiento del titular o poseedor, o el representante según el caso, del sistema informático, pues el Código Penal Paraguayo exige que el ataque se realice sin autorización, o teniéndola, en su exceso, como uno de los elementos constitutivos del referido tipo penal.

Por el contrario, si no hubiese existido consentimiento en la actividad desplegada por el hacker, si su acción fue para prevenir que otro realice un acceso indebido que esta por ocurrir, entonces si este actuante notifico los encargados la deficiencia del sistema informático con el fin de salvaguardar los datos y de lograr mejoras para el mencionado sistema, pues el análisis no prosperaría hasta la punibilidad por ser la conducta de este hacker no antijurídica, en el sentido del art 20 del C.P.:

> 1º No obra antijurídicamente quien, en una situación de peligro presente para un bien jurídico propio o ajeno, lesionara otro bien para impedir un mal mayor que no sea evitable de otra manera.
>
> 2º No obra antijurídicamente quien realizara el tipo legal de un hecho punible por omisión, cuando no podía ejecutar la acción sin violar otro deber de igual o mayor rango.

Basta que una persona detecte o padezca una intrusión para que se haga público el −hueco− para luego proteger para eventos futuros. Es decir, ello se tendrá en cuenta recién post juicio de antijuricidad de donde la proporcionalidad es el factor que daría la aprobación de la actividad del hacker ante un peligro presente.

Es más, él desde el ámbito de la informática ya se reconoce al −hacker

ético− (detección preventiva de debilidades), ni siquiera podría considerarse una amenaza, pues éstos estarían en colaboración, resguardo y mejoras de la ciberseguridad y en consideración a su actividad, al menos por ahora, de última, el derecho procesal es el que traería excepción de sanción para dichos casos a través, de las distintas salidas alternativas, como una colaboración y reconocimiento a la labor de estos técnicos que actúan en salvaguarda los datos que se hallan en los sistemas informáticos.

Marco legal de la Ley de Delitos Informático. Fortalezas y debilidades

Instituciones públicas que intervienen las actividades

Por el Poder Ejecutivo, se halla el CERT-PY, bajo la Dirección General de Políticas y Desarrollo de TICs de la Secretaría Nacional de Tecnología de la Información y de la Comunicación, SENATICs, creado por Decreto n.º 11.624/2013), se estableció el 30 de noviembre de 2012, con el objetivo de facilitar y coordinar la protección de los sistemas cibernéticos y de la información que respaldan la infraestructura nacional tanto gubernamental como del sector privado, así como garantizar una respuesta eficaz y oportuna a los incidentes cibernéticos. El CERT-PY ofrece servicios de difusión de boletines y noticias de ciberseguridad, auditorías de seguridad, respuesta a incidentes, análisis de malware, así como un canal de reporte de incidentes cibernéticos desde su portal, así como también a través de correo electrónico y redes sociales (Cert, 2016).

El Ministerio Publico, por Resolución de la Fiscalía General del Estado, F.G.E. n.° 3459/2010 creó la Unidad Especializada de Delitos Informáticos y amplía sus funciones por Resolución F.G.E. n.° 4408/2011, para hacer frente a aquellos hechos punibles que derivan del uso mal intencionado de la tecnología.

La iniciativa surge como respuesta a la necesidad de combatir de manera frontal y eficiente estos delitos. La Unidad tiene jurisdicción en todo el territorio nacional, es la principal autoridad a cargo de la investigación y de la acción judicial en casos de delitos informáticos, tales como alteración de datos en computadora, sabotaje de computadoras, operaciones fraudulentas por computadoras, alteración de datos relevantes para la prueba, entre otros.

Es importante resaltar que el Ministerio Público es la única autoridad gubernamental capaz de solicitar información a los prestadores de servicio internacionales cuando dicha información sea necesaria para una investigación. Por otro lado, el Código Procesal Penal, Ley n.° 1286/98, establece que cualquier persona conocimiento referente a un acto punible por parte del Estado deberá compartir dicha información con el Ministerio Público o con la Policía Nacional (Cert, 2016).

La presencia, así como la actividad desarrollada por los hackers genera polémica entre ellos mismos, el cuestionamiento surge a nivel mundial, pues, la problemática abarca intereses fundamentales. En el ámbito nacional también surge la disyuntiva entre los abogados y fiscales porque el Código Penal que regula los Delitos Informáticos no hace distinciones entre las intenciones de un hacker. Por ese motivo, no reconoce dicha figura en su carácter de colaborador voluntario, que aplica sus conocimientos de seguridad informática de un modo desinteresado para demostrar debilidades del sistema que pueda dar lugar a que otros hackers mal intencionados se filtre al sistema de seguridad con el fin de causar daño.

El comparativo más común en este tipo de conducta, es el ingreso a una vivienda ajena sin permiso previo, lo que significa hacer algo prohibido. Ahora

bien, en caso de contar con un permiso para ingresar con el fin de, detectar fallas de seguridad que pueda tener, la conducta es diferente. Se puede comparar con ésta casuística para una mejor comprensión, pues, sería como ir una casa ajena simplemente para demostrar lo fácil que es ingresar burlando la seguridad ¿es hecho punible? claro que sí, ya que la conducta no se toma con carácter preventivo.

Es necesario comprender los límites del nuevo derecho a la intimidad informática, como contrapunto del derecho al libre acceso a la información pública. El punto de quiebre entre ambos seria la vulneración a través del ataque o puesta en peligro de los datos informáticos protegidos jurídicamente.

Conclusión

Se puede afirmar que el avance de la tecnología a nivel global, trae consigo nuevas figuras delictivas que requieren de una normativa adecuada para la persecución de los hechos que generan, pues éstas, por lo general tienen una repercusión de carácter trasnacional.

La tendencia internacional actual en el ámbito legal prevé una regulación especial para atender estas conductas al considerarlas necesarias para la seguridad y protección de los bienes jurídicos vulnerables por este tipo de hechos punibles. Con ese fin, muchas legislaciones hacen una diferencia entre la función que cumplen los hackers, pues, existen otras intenciones entre un hacker ético y el no ético que se denomina *cracker*.

En este sentido, en la normativa nacional no permite esta regulación. Por lo tanto, en caso de que se quisiera el reconocimiento de los hackers éticos, se tendría que modificar los tipos penales en los cuales las normas prohíben dichas

conductas. Las funciones de los *hackers* éticos son punibles en el Paraguay, en el entendimiento de que el Estado protege y busca evitar toda posibilidad de invasión a la intimidad de las personas.

Se recomienda la regulación de esta figura a los efectos de contar con una ley que se adecue a esta modalidad de conducta, permita una organización para su implementación y pueda actuar de manera preventiva ante situaciones que signifiquen la vulneración de un sistema informático en el que se cuenta con datos e informaciones de carácter clasificado, tanto en el sector público como en el privado. En esa línea, se resalta la importancia de contar con el servicio de técnicos dependientes de la Secretaria Nacional de Tecnología de la Información, SENATIC que puedan detectar esas debilidades y por sobre todo que lo hagan de una manera legal y reglamentada.

Referencias

Constitución Nacional de 1992 de la República del Paraguay.

Código Procesal Penal de Paraguay, Ley n.° 1286/98

Código Penal paraguayo, Ley n.º 1.160/97

Ley n.° 3440/08, que modifica varios artículos de la Ley n.º 1.160/97

Ley n.° 4439/11, que modifica y amplia varios artículos de la Ley n.º 1.160/97

Abc Color. recuperado de: http://www.abc.com.py/nacionales/aumentaron-delitos-informaticos-1334874.html. Fecha: 07 de siembre de 2016. Asunción, Paraguay.

Abc Color. (8 de setiembre de 2016). Obtenido de http://www.abc.com.py/na-

cionales/sitio-web-para-robo-de-datos-emula-pagina-de-conocido-banco-439377.html

Centro de Respuestas ante Incidentes Cibertnètico, de la Secretarìa de TeC.N.ologìas de la Informaciòn y Comunicaciòn. Cert-Py. Recuperado de: https://www.cert.gov. py/index.php/certpy. Asunciòn, Paraguay.

Diccionario de la Lengua Española. Obtenido de Diccionario de la Lengua Española: http://dle.rae.es/?id=T8ktrp2. Fecha de revisiòn: (5 de setiembre de 2016)

Portal Oficial del Gobierno fue Hackeado. Diario ûltima Hora. Fecha de publicaciòn: 23 de mayo de 2013). Recuperado de: http://m.ultimahora.com/portal-oficial-del-gobierno-fue-emhackeadoem-n621960.html. Asunciòn, Paraguay

Schöne, W. Recuperado de: https://www.unifr.ch/ddp1/derechopenal/articulos/a _20080527 _08.pdf. Fecha de revisiòn: 5 de setiembre de 2016.

Ministerio Público, página Web oficial. Recuperado de: www.ministeriopublico.gov.py. Fecha: 08 de setiembre de 2016.

Moderno Discurso Penal y nuevas tecnologías. Memorias III Congreso Internacional de jóvenes investigadores en Ciencias Penales. Salvadori, 2013, pág. 119. Edición 2013. Editorial Aquílafuente. Salamanca, España.