Delitos informáticos. Modalidades delictivas. Legislación actual y anteproyecto del Código Penal

Dr. Gustavo Pérez de Urrechu
Juez Penal de 1era Instancia de Distrito Nro 2, Rosario.

Introducción

Dos titulares: «Los Hackers ahora se meten en los celulares y amenazan a sus dueños» y «Numerosos países pinchan los teléfonos»[1]. Anverso y reverso de la misma moneda: el impacto de las nuevas tecnologías de la comunicación e información (TIC). En el primer caso, particulares u organizaciones delictivas que despliegan prácticas, utilizando medios informáticos que afectan a particulares, provocando la obstrucción de los servicios telefónicos e informáticos. En el segundo, el avance de los estados en el ámbito privado, desplegando una vigilancia solapada, superando con sutileza lo imaginado por George Orwell al observa a la sociedad inglesa en el año 1948 y que plasmara en su reconocida novela de ciencia ficción «1984».

Así, varias décadas atrás estas tecnologías estaban en la imaginación de autores de ciencia ficción como Isaac Asimov, Ray Bradbury, o Philip K. Dick, entre otros, e inspiraron a las generaciones que les precedieron, la creación de las computadoras, internet, los teléfonos celulares, por mencionar algunos inventos, que hoy son una realidad, realidad que es cada vez más vertiginosa, con cada vez menos tiempo de recambio entre una nueva generación tecnológica, que va dejando obsoletas las anteriores, y a cada uno de nosotros, con una sensación de agobio, ya que cuando comenzamos a familiarizarnos una tecnología, ya rápidamente cambian los equipos (hardware) y mucho más rápido los programas (software).

Los cambios en las TIC se han dado en los más variados ámbitos del ser humano, tanto sea el estatal, comercial, industrial, financiero y particular, modificándolos sustancialmente.

El desarrollo de tales tecnologías, que en un comienzo estaba reservada para ámbitos militares, científicos y académicos, hoy se han masificado en la sociedad global, principalmente por el uso de Internet.

Estos cambios han impactado no por el hecho de que antes no hubiera comunicaciones e información, sino que los avances científicos en la materia han permitido detectar, captura, analizar y correlacionar datos, los cuales hoy pueden ser utilizados con las más variadas finalidades, siendo una de ellas, la delictiva.

Este fenómeno representa todo un desafío para los operadores del derecho y sus tiempos, ya que la dinámica de estas nuevas tecnologías, daría la impresión de que siempre se llegando tarde y no se dan respuestas.

Como señaláramos, uno de los principales cambios se ha dado en la sociedad global. Señalan Nieto Martín, Adán y Maroto Calatayud, Manuel[2], que «la sociedad ha mutado desde una forma disciplinaria, que describiera Foucault y que nace con la Ilustración, a una que podemos denominar de «sociedad de control». En la sociedad disciplinaria los individuos eran vigilados dentro de una institución (familia, cárcel, escuela, ejército, fábrica). En las sociedades de control, la vigilancia es ubicua, ocupa todos los espacios de la vida pública y privada. En el modelo panóptico de vigilancia foucaultiano el individuo sabía que era vigilado; en la sociedad de control, gracias a esta ubicuidad de la vigilancia, el ciudadano olvida que es vigilado, o no le importa, pues la vigilancia va implícita en tareas tan cotidianas como navegar por internet, utilizar su smartphone, entrar en un establecimiento donde hay instalada una cámara de vigilancia, pagar en él con la tarjeta de crédito o pasar el control de seguridad del aeropuerto»; y tal situación se ha visto potenciada luego del atentado de las torres gemelas el 11.9.2001, y la aparición de nuevas formas de gobierno (estado vigilante), en una nueva etapa del capitalismo (postfordista o posindustrial).

Hoy, todos nosotros tenemos un pasado digital, que no se borra nunca. Se va construyendo cada vez que nos documentamos, viajamos al exterior, usamos una tarjeta de transporte, operamos un cajero automático, realizamos una compra con tarjeta de crédito o débito, o cuando hacemos una búsqueda en Google o más puntualmente en alguna red social como Facebook, datos de su vida privada, sus intereses, gustos, ubicación, sube a la nube fotos, se genera información que es recolectada (minería de datos

o data mining) por los operadores públicos y privados (comunicaciones e informaciones de bancos, financieras, aseguradoras, empresas de comunicaciones, televisión, internet que tienen un gran valor económico), con diversos fines, como ser marketing (v.gr. para licitar publicidad, en el caso Google), cruzamiento de datos fiscales o seguridad.

Como señala Stefan Gross Selbeck, «los datos personales son el petróleo del siglo XXI»[3].

Un aspecto preocupante, por la creación de perfiles (profiling), es cuando la valoración de dichos datos es negativa y lleva a la conformación de listas negras por estereotipos peligrosistas.

En tal contexto, por la vertiginosa dinámica de la realidad descripta, nos encontramos que no ha variado el modelo del estado, ello trae como lógica consecuencia que los diferentes poderes del estado, a través de estructuras heredadas de otra realidad, reaccionaran y reaccionen tardíamente.

Así, se ve en la demora para legislar sobre delitos informáticos, generando vacíos legales, incertidumbre e impunidad, a lo cual se agrega las dificultades del accionar del poder de policía estatal a la hora de perseguir la «ciberdelincuencia» ya sea por falta de capacitación y de medios en algunas agencias, o la transgresión de las garantías del ciudadano, por el avance selectivo del poder punitivo en manos de agencias que cuentan y concentran recursos para tales fines.

Una barrera importante de la ciencia jurídica para abordar este fenómenos es cuando queremos «aplicar principios y conceptos de un mundo con fronteras físicas al fenómeno de la información en internet que no tiene fronteras»[4], para dar respuesta a la afectación de las garantías fundamentales del ciudadano frente al avance de agencias públicas y/o privadas, o por organizaciones o simples particulares que invaden la esfera de intimidad, la libertad, seguridad o la afectación al patrimonio.

Mas no debemos apartarnos de un pilar fundamental como es el respeto al principio de legalidad. La conducta debe estar, tipificada (cada acto ilícito para que sea delito debe formar parte de la normativa penal. Si no es así, se entra en un «vacío legal».

En el presente artículo, dado lo extenso del tema, tratará a grandes trazos las prácticas relevantes detectadas en la ciberdelincuencia, los sujetos activos y la legislación actual y el anteproyecto de código penal.

Sujetos y modalidades Delictivas [3y5]

Sintéticamente, y a los fines ilustrativos, transcribimos los términos técnicos más utilizados para definir a los sujetos activos involucrados, los programas que utilizan y las maniobras delictivas.

En el ámbito de la informática, las personas que realizan determinadas prácticas son conocidos como:

Hacker: son especialistas en tecnologías de la información y telecomunicaciones en general, aunque actualmente, se utiliza este término para referirse a aquellos que utilizan sus conocimientos con fines maliciosos como el acceso ilegal a redes privadas. Según algunos expertos, es incorrecto asociar éste término únicamente con aquellas prácticas fraudulentas, ya que existen dos tipos de hackers: los «White Hat», que son especialistas en informática que utilizan sus conocimientos con el fin de detectar cualquier tipo de vulnerabilidad, errores o fallos de seguridad, etc. para poder solucionarlos y evitar posibles ataques y los «Black Hat» o «Cracker»: expertos en seguridad informática que tratan de detectar las debilidades o deficiencias de programas y equipos informáticos, para obtener algún tipo de beneficio (obtener información, distribuir virus, introducirse ilegalmente en redes, eliminar la protección anticopia del software comercial, burlar la seguridad de determinados sistemas informáticos).

Lammers: son hacker de poco conocimiento, que dañan por placer.

Programas y técnicas informáticas

Crimeware: son todos aquellos pro-

gramas informáticos diseñados para obtener beneficios económicos, mediante la comisión de todo tipo de delitos online. Se considera crimeware el phishing, spam, adware, etc.

Malware: (Acrónimo en inglés de: «Malcious software» engloba a todos aquellos programas "maliciosos" (troyanos, virus, gusanos, etc.) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al sistema informático o al usuario del mismo.

Adware: utilizados para difundir publicidad (banners, ventanas emergentes) pueden funcionar como spyware o espía, al capturar información sobre los hábitos de navegación del usuario sin su consentimiento.

Backdoor: puerta trasera dejada por el programador para acceder al programa, por una secuencia especial en el código de programación, los cuales son potenciales problemas de seguridad ante el accionar de los hackers.

Troyano: programa ejecutable que aparenta realizar una tarea determinada, para engañar al usuario, con el fin de llevar a cabo acciones como controlar el equipo informático, robar información confidencial, borrar datos, descargar otro tipo de malware, etc. La principal diferencia entre los troyanos y los virus es que los troyanos no pueden replicarse a sí mismos.

Bomba lógica: programa que se instala en un equipo ajeno, que está inactivo hasta que se activa y el programa comienza a llevar a cabo las acciones para las que ha sido diseñado, que pueden ser: ordenar que se realice una transferencia bancaria, dañar el sistema, borrar datos del disco duro.

Exploit: programa que aprovecha las fallos de seguridad, defectos o vulnerabilidades de otros programas o sistemas informáticos, con el fin de obtener algún tipo de beneficio o de llevar a cabo una acción concreta, como acceder a recursos protegidos, controlar sistemas sin autorización, etc.

Spoofing: programas para ocultar y suplantar direcciones IP.

Screen recorders: programas utilizados para captura de pantallas presentadas al usuario.

Sniffer: programa espía que intercepta y retransmite las informaciones que circulan en las redes internas.

Virus: Código informático que se replica a sí mismo y se propaga de equipo en equipo por medio de programas o archivos a los que se adjunta. Para que se produzca la infección, es necesaria la intervención humana, es decir, el usuario debe realizar algún tipo acción como enviar un correo o abrir un archivo. Se utilizar para la alteración, el daño o la destrucción del equipo o sistema informático, de su información y programas.
Gusano o Worms: programas con características similares a las de los virus, aunque a diferencia de los éstos, son capaces de realizar copias de sí mismos y propagarse, a través de la red para infectar otros equipos, sin la intervención de un usuario. Una de las formas más habituales de propagación de gusanos es el envío masivo de correos electrónicos a los contactos de las libretas de direcciones de los usuarios.

Dialers: programa que se instala en un equipo con el fin de modificar los datos de acceso a internet, para que al realizar la conexión a través de un módem, se utilice un número de tarificación adicional (Los números de tarificación adicional o NTA son aquellos cuyo coste es superior al de una llamada nacional, por ejemplo aquellos que empiezan por prefijos como 806, 907, etc.). La utilización de dialers o marcadores telefónicos es lícita si se informa al usuario de los costes, se le avisa del la redirección de la conexión y si se instala el programa con su consentimiento.

Spyware o Programa Espía: su objetivo es recopilar información del usuario del sistema en el que se instala. Los datos que se recogen suelen estar relacionados con los hábitos de navegación del usuario y se utilizan con fines publicitarios. Aunque la instalación de los programas espías puede realizarse con el consentimiento expreso del usuario, en muchos casos, se instalan sin la autorización de éste, al instalar otro programa supuesta-

mente inofensivo, o mediante virus o un troyanos, distribuidos por correo electrónico.

Firewall o cortafuegos: mecanismo de seguridad que regula el acceso entre dos o más redes, teniendo en cuenta la política de seguridad establecida por la organización responsable de la red. Habitualmente se utilizan los cortafuegos para proteger redes internas de accesos no autorizados.

Flood o flooder: Programa que se utiliza para enviar mensajes repetidamente y de forma masiva, mediante correo electrónico, sistemas de mensajería instantánea, chats, foros, etc. El objetivo de este comportamiento es provocar la saturación o colapso de los sistemas a través de los que se envía el mensaje.

Keylogger: Programa o dispositivo que registra las combinaciones de teclas pulsadas por los usuarios, y las almacena para obtener datos confidenciales como contraseñas, contenido de mensajes de correo, etc. La información almacenada se suele publicar o enviar por internet.

Modalidades delictivas

Ataques por saturación: el sistema es bombardeado con cuestiones falsas, logrando saturarlo y bloquearlo. Recibe el nombre de mailbombing, cuando utilizando programas denominados flood o flooder, se envían muchos mensajes para bloqueo de los emails.
Ciberchantaje: amenaza de activar bombas lógicas.

Ciberescuchas: intercepción de emails por líneas telefónicas.

Cracking: vulneración de claves.

Hacking: ataque intencional perpetrado contra sistemas de información.

Pharming: Modalidad de estafa online que utiliza la manipulación de los servidores DNS (Domine Name Server) para redireccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales del usuario, como contraseñas, datos bancarios, etc.

Spam: envío masivo de mensajes no solicitados, con contenido generalmente publicitario, que se realiza a través de distintos medios como: foros, mensajería instantánea, blogs, etc. aunque el sistema más utilizado es el correo electrónico. Para obtener la lista de direcciones de correo, los spammers o remitentes de "mensajes basura", emplean software especializado o robots que rastrean páginas web en busca de direcciones, compran bases de datos, utilizan programas de generación aleatoria de direcciones, copian las direcciones de listas de correo. Cuando es por red inalámbrica se denomina warspamming.

Pirateo de web: modificación a distancia del contenido de páginas web.

Phreaking o Pirateo de línea telefónica.

Carders sustracción informática de tarjetas.

Hijacking: técnicas informáticas que se utilizan para adueñarse o «secuestrar» páginas web, conexiones de internet, dominios, IPs, etc.

Hoax: mensaje de correo electrónico con información engañosa, que pretende avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Los hoaxes se caracterizan por solicitar al destinatario que reenvíe el mensaje a todos sus contactos, así logran captar las direcciones de correo de usuarios a los que posteriormente se les enviarán mensajes con virus, spam, phishing, etc.

Phishing: maniobra defraudatoria a través de internet, que pretende conseguir datos confidenciales de usuarios (contraseñas o claves de acceso a cuentas bancarias). Se realizan envíos masivos de correos electrónicos, simulando proceder de entidades de confianza, donde se pide al usuario que, por «motivos de seguridad» o con el fin de «confirmar su cuenta", facilite sus datos. Puede solicitarse los datos en el mismo mensaje o que los ingrese en la página web de la entidad en cuestión, que es una copia idéntica de la original.

Scam o Phishing Laboral: Fraude similar al phishing, con el que comparte el objetivo de obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias. Consiste en el envío masivo de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen supuestos empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.

SmiShing: Es una variante del phishing, que utiliza los mensajes a teléfonos móviles, en lugar de los correos electrónicos, para realizar el ataque. El resto del procedimiento es igual al del phishing: el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falseada, idéntica a la de la entidad en cuestión.

Spear Phishing: Tipo de phishing en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional.

Vishing: Fraude que persigue el mismo fin que el Phishing: la obtención de datos confidenciales de usuarios, pero a través de un medio distinto: la telefonía IP. Los ataques de vishing se suelen producir siguiendo dos esquemas: a) Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita, b)Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etc.

Particularidades de los delitos informáticos

Las TIC han generado y seguirán generando debates en la doctrina y jurisprudencia, dado la aparición de nuevos medios electrónicos o informáticos, cuál es el tratamiento que requieren y cuál es su receptación legal.

En pocas palabras, queremos remarcar las dificultades en el marco del derecho, y en particular del derecho penal, de lograr dar respuesta a los rápidos avances de las TIC's, y de nuevas tecnologías, tanto si se usan como método, medio o si son objeto del delito.[6]

Una de las últimas reformas del código penal, se ha incorporado el grooming (art. 131 C.P.). Aquí vemos que se penaliza cualquier delito contra la integridad sexual de una persona menor de edad, y lo es por el medio empleado empleado (referencia de medios: comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos).

En cuanto a los términos empleados por el legislador, se buscan referencias que no queden desactualizadas por el avance tecnológico. Por ejemplo en los delitos de violación, obstrucción, desvío y/o publicación de e-mails y conversaciones de mensajería electrónica. Este último término mensajería electrónica engloba no son solo correos electrónicos, sino todo lo que circula a través de un medio electrónico, e incluye whasapp, chat, BBM, y todos los que vayan apareciendo.

Otro claro ejemplo que cabe mencionarse, la dificultad de conciliar los tradicionales elementos de la estafa y la aparición de tecnología donde no interviene un ser humano. En el caso en que el «agente manipula la información para obtener un rédito económico habían sido tipificados -alternativamente- como hurto o como estafa, y no faltaron fallos que los tuvieron por atípicos», y ya en relación al actual art. 173 inc. 16 del C.P. lo que hace particular el delito es que no concurre el error en ninguna persona física.... «Buompadre advierte que de la tipificación de esta conducta no debe concluirse que ha variado los elementos de la estafa o que se han flexibilizado sus requisitos típicos, solo se trata de una figura especializada por el medio empleado»[7].

Otro caso interesante para apreciar la problemática de estos delitos, es el de los pescadores. Estos mecanismos son utilizados para captar las tarjetas que luego podrán ser utilizadas ilícitamente o para sustraer billetes, mediante la utilización de bandas engomadas que se colocan y bloquean la boca de expendio del dinero, quedando los billetes atrapados por estas bandas engomadas, las cuales son retiradas, junto con el dinero. Los tipos penales refieren a la defraudación con la utilización de tarjetas de compra, crédito o débito (art. 173 inc. 15 C.P.) y no surge ningún tipo de manipulación informática (art. 173 inc. 16 C.P.); conforme la legislación actual, configurarían el delito de hurto (art. 162 C.P.).[8]

En cuanto a la alteración normal del normal funcionamiento y/o interrupción de los sistemas de información o de las comunicaciones, también se generan problemas, ya que hay diferentes formas de interrumpir las comunicaciones y al no estar tipificado, es un problema para los que manejan sistemas de información, dado que podemos tener interrupciones ajenas a propósito y no sigue siendo un delito.[9]

Clasificación de los delitos informáticos [6 y 10]

Como Método: los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como Medio: para realizar un delito utilizan una computadora como medio o símbolo.

Como Fin: son dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Legislación vigente en materia de delitos informáticos

1) Ley 26.904: «Ley de Grooming» o Ciberacoso Sexual (incorpora el art. 131 al Código Penal). Extorsión a través de la confianza de los chicos a hacer cosas que luego aparecen en sitios de pornografía.
2) Ley 26.388: Modificación del Código Penal (B.O. 25 de junio de 2008)
*Distribución y/o tenencia de pornografía infantil
*Violación, obstrucción, desvío y/o publicación de e-mails y conversaciones de mensajería electrónica.
*Acceso indebido a bases de datos privados
*Acceso indebido a perfiles de redes sociales
*Acceso indebido a documentación personal
*Alteración normal del normal funcionamiento y/o interrupción de los sistemas de información
Interrupción de las comunicaciones.
*Daño informático, inutilización, modificación y/o eliminación
*Venta, introducción o distribución de virus.
3) Ley 25.930: Modificación del Código Penal. Defraudación mediante tarjeta de compra, crédito o débito (art. 173 inc. 15)
4) Ley 25.326: Ley de Protección de los Datos Personales.
5) Ley 21.766: Falsificación de documentos. Nómina de documentos equiparados a aquellos que acreditan identidad de las personas. Modifica al Código Penal

Nuevo Anteproyecto de Código Penal[9]

En términos generales, se conserva el delito de grooming, bajando la edad de los menores a 13 años; se quita la figura de la tenencia de material pornográfico con fines de distribución o comercialización, se conservan los delitos relacionados con las comunicaciones electrónicas, los accesos ilegítimos y el fraude en su modalidad informática; se incorpora también el sustracción de identidad, mas no el ataque por denegación de servicio. [11]
Acciones privadas. Acceso ilegítimo a la información y delitos contra el honor (art. 44). Definiciones de información privilegiada, firma digital, certificado digital, documento, dato informático, tráfico de comunicación y discriminación (art. 63)
Calumnias e injurias. Incluso recíprocas (art. 100, 103 y 104)
Publicación y/reproducción (art. 101)
Amenazas (art. 115)
Violación, intercepción, supresión y/o desvío de comunicaciones de cualquier tipo (art. 119)
Violación a la privacidad (art. 120)
Comunicación pública o indebida. Re-

producción de tal (art. 121)
Secreto profesional y funcional que genere daños a terceros (art. 122)
Acceso ilegítimo a la información. Más aún si es pública (art. 123)
Suplantación de identidad (art. 123)
Pornografía infantil, producción, tenencia y reproducción (art. 131)
Exhibiciones obscenas a menores (art. 132)
Extorsión (art. 142)
Estafa (art. 143)
Defraudaciones y estafas informáticas (art. 144)
Violación de derechos intelectuales (art. 150)
Falsificaciones y usos de marcas (art. 151)
Daño o destrucción informática (art. 160)
Interrupción de servicio (art. 190)
Intrusión a la defensa nacional (art. 222)
Inutilización de pruebas (art. 260)
No punibles. Actúan en cumplimiento de un deber jurídico (art. 5).
Supuestos de no punibilidad: cónyuges o ascendientes y descendientes en línea recta. Viudos y/o difuntos cónyuges (art. 162)

Conclusión

Las TIC generan un gran desafío en punto a la legislación penal, tanto frente al accionar de sujetos particulares como los crackers, como frente al avance de las agencias estatales.

Esto implica que los operadores penales debe redoblar sus esfuerzos para lograr que las nuevas modalidades delictivas en torno a la pornografía infantil, estafas, violación de comunicaciones, sustracción de información, por mencionar algunas conductas ilícitas, sean debidamente captados por la legislación respetando así el postulado «nullum crimen, nulla poena sine lege praevia, scripta, stricta et certa», que prohíbe las penas sin ley, y sin ley previa, escrita y estricta, además de ser precisas y determinadas, previsto por el art. 18 de la C.N. « Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso»[12], dado que el avance de las tecnologías llevan a que el legislador llegue tarde y nos encontremos con conductas que no sean delitos por más que los fines sean ilícitos.

Además, hoy el Estado cuenta con la capacidad de poder acceder a una mayor cantidad de información de calidad y su análisis, por lo que el derecho penal debe propender a limitar el avance de su poder punitivo, y el respeto de los derechos fundamentales, como ser la salvaguarda de la esfera privada del ser humano, conforme el principio de reserva (art. 19 C.N.).

Ello no significa que el Estado no pueda generar políticas persecutorias del delito en base al análisis de la información, sino que dicha información debe ser prudentemente utilizada a fines de no caer en prácticas totalitarias.

En cuanto a la legislación actual, desde la ley 26388, pasando por la incorporación del Grooming, nuestro país ha implementado los lineamientos del Convenio de Budapest, agiornando su legislación a la nueva realidad de las TIC`s.

La comisión que conformó el Anteproyecto de Código Penal ha seguido ese lineamiento, proponiendo algunas mejoras a la legislación actual.

En tal sentido, aportes de los especialistas en la materia giran discutir la baja de la edad de los menores a 13 años en la figura de Grooming, la derogación de la figura de la tenencia de material pornográfico con fines de distribución o comercialización, y que no se ha legislado el ataque por denegación de servicio (DDOS).

Sobre este último punto, los crackers utilizar virus que funcionan como «zombies»: se les da la orden que despierten y ataquen el servidor, que no puede responder ante los múltiples pedido y se bloquea y luego la red de ese servidor, no pudiendo contar con el servicio contratado.

Se discute la falta de regulación de la responsabilidad de los usuarios por la falta de idoneidad y el uso descontrolado de la tecnología, ni de los proveedores de internet (ISP) ni de los proveedores de hosting ni de dueños de servidores, o la regulación de conducta ilícitas en el ámbito laboral, para empleadores y empleados.

Finalmente, dejar sentado como política de discusión sobre el tema de los delitos informáticos para la necesaria captación de este fenómeno, un prudente análisis inter-disciplinario tecnológico/jurídico y de seguridad informática para tipificar las posibles conductas disvaliosas en nuestro país. ■

Bibliografía

• Riquert, Marcelo Alfredo, Informática y Derecho Penal Argentino, 1999, Ad hoc.

• Valli, Gabriela, Los delitos informáticos y la evidencia digital. Revista del Colegio de Magistrado y Funcionarios del Poder Judicial de la Provincia de Santa Fe, N° 3, pág. 519.

• Altmark, Daniel Ricardo y Molina Quiroga, Eduardo, Tratado de Derecho Informático, Tomo III, Editorial La Ley, 2012

• Palazzi, Pablo A., Los Delitos Informáticos en el Código Penal. Análisis de la ley 26338. 1a Edición, Buenos Aires, AbeledoPerrot, 2009.

• Delle Donne Carla, Un nuevo análisis de la responsabilidad penal de los intermediarios en internet: el tercer procesamiento en la causa contra los administradores de taringa. net, Derecho Penal y Procesal Penal, N° 5, mayo 2013, Editorial AbeledoPerrot.

• Riquert, Marcelo. El convenio de Budapest y el Mercosur: estado de la legislación latinoamericana sobre cibercriminalidad, pág. 137, Revista de Derecho Penal y Criminología, año III, N° 10, noviembre 2013, Editorial La Ley.

• Riquert, Marcelo, Gutiérrez, Ricardo y

Radesca, Laura, El delito de acceso ilegítimo a sistema o dato informático (intrusismo informático simple), Revista de Derecho Penal y Criminología, año III, N° 11, diciembre 2013, pág. 109, Editorial La Ley.

• Cueto, Mauricio, Grooming: el nuevo artículo 131 del Código Penal, Revista de Derecho Penal y Criminología, N° 2, marzo 2014, pág. 44, Editorial La Ley.

• Riquert, Marcelo, El nuevo tipo penal de «cibergrooming» en Argentina, Revista de Derecho Penal y Criminología, N° 1, febrero 2014, pág. 21, Editorial La Ley

• Diaz Cortés, Lina Mariola, El nuevo delito de child grooming en España: realidad criminológica y respuesta penal, Revista de Derecho Penal y Criminología, N° 7, agosto 2011, pág. 75, Editorial La Ley

• Delle Donne Carla y Pablo A. Palazzi, Delincuencia online que afecta menores: el grooming tipificado como corrupción de menores agravada, Derecho Penal y Procesal Penal, n° 2, Febrero 2014, Editorial AbeledoPerrot.

• Donna Edgardo, El código Penal y su interpretación en la jurisprudencia, Tomo IV, pág. 113 (art. 173 inc. 15 y 16 C.P.)

• Anteproyecto de Código Penal de la Nación. 1° edición. 2014, Editorial del Ministerio de Justicia y Derecho Humano de la Nación.

• Carles, Roberto, Cuadro cuadro comparativo. Penas del Código Penal Vigente y penas propuestas por la Comisión para la Elaboración del Proyecto de Ley de Reforma, Revista de Derecho Penal y Criminología, año IV, N° 4, mayo 2014, pág. 207, Editorial La Ley.

Notas

[1] Diario La Capital de Rosario. Edición impresa. 7.6.2014

[2] Nieto Martín, Adán y Maroto Calatayud, Manuel, Las redes sociales en internet como instrumento de control penal. Tendencias y Límites. Revista de Derecho Penal y Criminología, N° 1, febrero 2013, pág. 93, Editorial La Ley.

[3] Zarich, Faustina, Delitos Informáticos. Seguridad en internet. Conferencia brindada en la ciudad de Santa Fe, el 4.6.2013, en el Centro de Capacitación Judicial de la Corte Suprema de Justicia de la Provincia de Santa Fe.

[4] Salt, Marcos, Nuevos desafíos de la evidencia digital. El acceso transfronterizo de datos en los países de américa Latina. Derecho Penal y Procesal Penal N° 6, junio 2013, pág. 1132. Editorial AbeledoPerrot.

[5] Glosario http://delitosinformaticos.info/delitos_informaticos/glosario.html

[6] Lima de la Luz, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984.

[7] D'Alessio, Andrés. Código Penal comentado y anotado: 2da edición actualizada y ampliada. Bs. As. 2009, Tomo 2, pág. 753.

[8] Amelotti Nicolás, Quien coloca un pescador en la boca de un cajero automático para apoderarse de dinero ¿puede ser considerado autor mediato del delito tipificado en el artículo 173 inciso 15, Cpen? Derecho Penal y Procesal Penal n° 2, febrero 2013, pág. 229. Editorial AbeledoPerrot

[9] Mansueti, Marcos. Delitos informáticos. http://www.youtube.com/watch?v=rGt_omNCn2s

[10] Salt, Marcos. Delitos Informáticos de carácter económico. P. 225 en Delitos no convencionales. Editores del Puerto, 1994

[11] Dr. Ricardo Saenz, http://delitosinformaticos.fiscalias.gob.ar/actualidad/reforma-del-codigo-penal/

[12] Zaffaroni, Eugenio Raúl, Slokar, Alejandro y Alagia, Alejandro, Derecho Penal, parte general, pág. 110