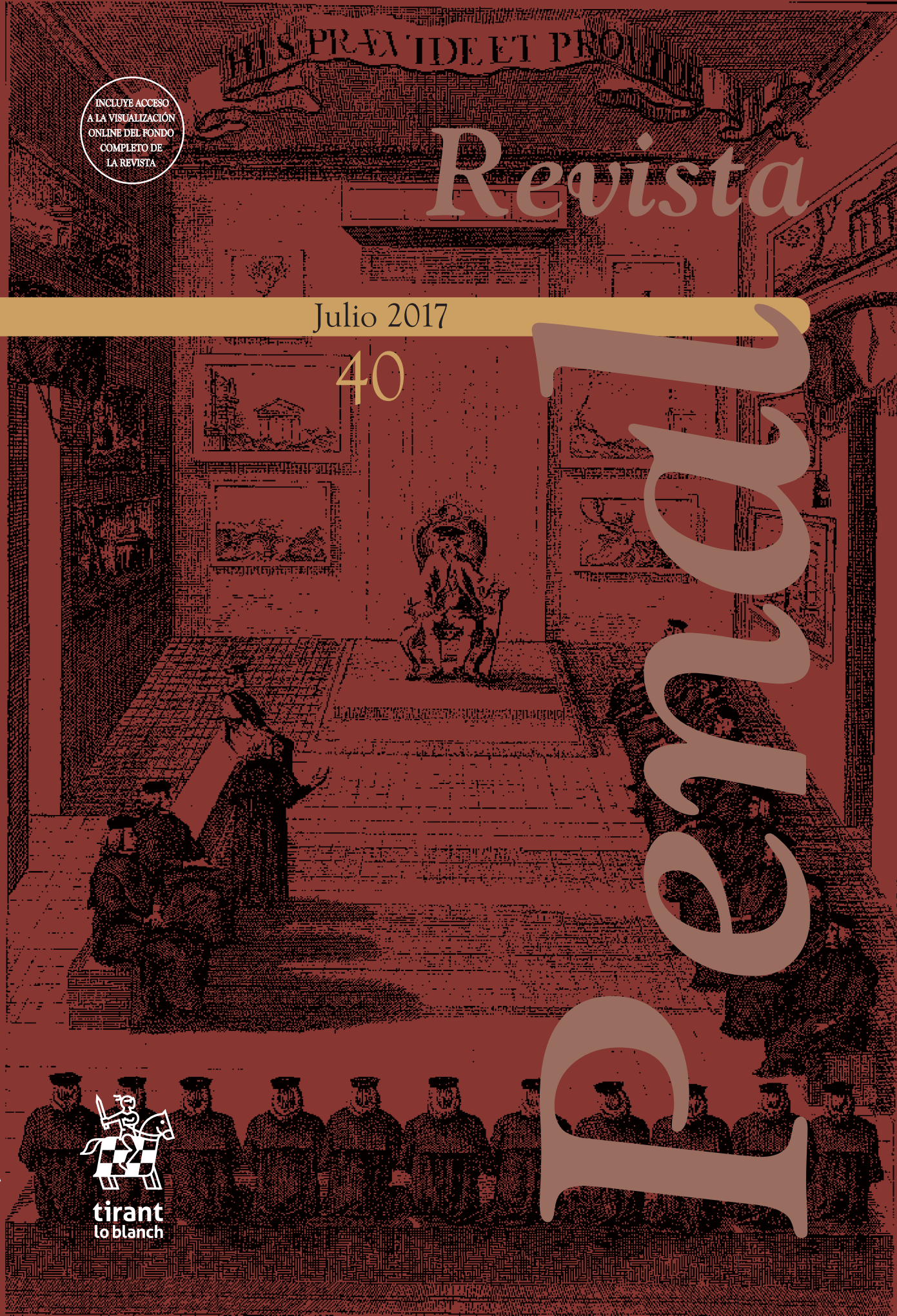
40

INCLUYE ACCESO A LA VISUALIZACIÓN ONLINE DEL FONDO COMPLETO DE LA REVISTA

Revista Penal

Julio 2017

40



Revista Penal

Julio 2017

tirant lo blanch

tirant lo blanch

Revista Penal

Número 40

Sumario

Doctrina:

– Delito y solidaridad (estado de necesidad, omisión del deber de socorro y bienes jurídicos colectivos de solidaridad), por *Mercedes Alonso Álamo* 5
– Política criminal contra la corrupción: la reforma del decomiso, por *Ignacio Berdugo Gómez de la Torre*..... 22
– "Conditio sine qua non" y concreción del riesgo en el resultado: cómo eliminar un paso repetitivo en el análisis de la imputación objetiva al tipo, por *Patricia Esquinas Valverde* 43
– Cuidados paliativos: ¿eutanasia o asistencia sanitaria? Un análisis desde los conceptos, por *Javier García Amez* 77
– Juicios rápidos y conformidad: la posible vulneración de los derechos fundamentales, por *Marta García Mosquera* 97
– Organización criminal para la financiación ilegal de un partido político: el "caso de los papeles de Bárcenas", por *Nicolás García Rivas* 111
– Función y fines de la pena: la ejecución de penas privativas de libertad en el caso de los delincuentes de cuello blanco, por *Carmen Juanatey Dorado* 126
– ¿A qué "partido político" imputar y eventualmente condenar?, por *José León Alapont* 146
– La interpretación del término "población civil" como elemento del tipo en el crimen contra la humanidad, por *Alfredo Liñán Lafuente* 168
– La falsedad en las cuentas en la legislación italiana: la última reforma y las nuevas cuestiones interpretativas, por *María Novela Masullo* 183
– Derecho penal, Criminología y política criminal en la era del punitivismo, por *Manuel Portero Henares* 193
– El delito de maltrattamenti contro familiari e conviventi en el Código Penal italiano, por *Bárbara San Millán Fernández* 210
– El blanqueo de capitales como norma de flanqueo invertida (una posible interpretación sobre su naturaleza jurídica), por *Lorena Varela* 236

Sistemas penales comparados: Delitos informáticos (Cybercrimes) 250

tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, Pablo Olavide de Sevilla y la Cátedra de Derechos Humanos Manuel de Lardizábal.

Dirección

Juan Carlos Ferré Olivé. Universidad de Huelva
jcferreolive@gmail.com

Secretarios de redacción

Víctor Manuel Macías Caro. Universidad Pablo de Olavide
Miguel Bustos Rubio. Universidad Internacional de La Rioja

Comité Científico Internacional

Kai Ambos. Univ. Göttingen
Luis Arroyo Zapatero. Univ. Castilla-La Mancha
Ignacio Berdugo Gómez de la Torre. Univ. Salamanca
Gerhard Dannecker. Univ. Heidelberg
José Luis de la Cuesta Arzamendi. Univ. País Vasco
Albin Eser. Max Planck Institut, Freiburg
Jorge Figueiredo Dias. Univ. Coimbra
George P. Fletcher. Univ.Columbia
Luigi Foffani. Univ. Módena
Nicolás García Rivas. Univ. Castilla-La Mancha
Vicente Gimeno Sendra. UNED
José Manuel Gómez Benítez. Univ. Complutense
Carmen Gómez Rivero. Univ. Sevilla
José Luis González Cussac. Univ. Valencia
Borja Mapelli Caffarena. Univ. Sevilla
Victor Moreno Catena. Univ. Carlos III
Francisco Muñoz Conde. Univ. Pablo Olavide
Enzo Musco. Univ. Roma
Francesco Palazzo. Univ. Firenze
Teresa Pizarro Beleza. Univ. Lisboa
Claus Roxin. Univ. München
José Ramón Serrano Piedecasas. Univ. Castilla-La Mancha
Ulrich Sieber. Max Planck. Institut, Freiburg
Juan M. Terradillos Basoco. Univ. Cádiz
Klaus Tiedemann. Univ. Freiburg
John Vervaele. Univ. Utrecht
Eugenio Raúl Zaffaroni. Univ. Buenos Aires
Manuel Vidaurri Aréchiga. Univ. La Salle Bajío

Consejo de Redacción

Miguel Ángel Núñez Paz y Susana Barón Quintero (Universidad de Huelva), Adán Nieto Martín, Eduardo Demetrio Crespo y Ana Cristina Rodríguez (Universidad de Castilla-La Mancha), Emilio Cortés Bechiarelli (Universidad de Extremadura), Fernando Navarro Cardoso y Carmen Salinero Alonso (Universidad de Las Palmas de Gran Canaria), Lorenzo Bujosa Badell, Eduardo Fabián Caparros, Nuria Matellanes Rodríguez, Ana Pérez Cepeda, Nieves Sanz Mulas y Nicolás Rodríguez García (Universidad de Salamanca), Paula Andrea Ramírez Barbosa (Universidad Externado, Colombia), Paula Bianchi (Universidad de Los Andes, Venezuela), Elena Núñez Castaño (Universidad de Sevilla), Carmen González Vaz (Universidad Complutense) Pablo Galain Palermo (Max Planck Institut - Universidad Católica de Uruguay), Alexis Couto de Brito y William Terra de Oliveira (Univ. Mackenzie, San Pablo, Brasil).

Sistemas penales comparados

Martin Paul Wassmer (Alemania)
Luis Fernando Niño (Argentina)
Alexis Couto de Brito (Brasil)
Jia Jia Yu (China)
Álvaro Orlando Pérez Pinzón (Colombia)
Roberto Madrigal Zamora (Costa Rica)
Elena Núñez Castaño (España)
Angie Andrea Arce Acuña (Honduras)
Manuel Vidaurri Aréchiga (México)
Sergio J. Cuarezma Terán (Nicaragua)
Carlos Enrique Muñoz Pope (Panamál)
Víctor Roberto Prado Saldarriaga (Perú)
Svetlana Paramonova (Rusia)
Volodymyr Hulkevych (Ucrania)
Pamela Cruz/Sofía Lascano (Uruguay)
Jesús Enrique Rincón Rincón (Venezuela)

www.revistapenal.com

© TIRANT LO BLANCH
EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
IMPRIME: Guada Impresores, S.L.
MAQUETA: Tink Factoría de Color

Si tiene alguna queja o sugerencia envíenos un mail a: *atencioncliente@tirant.com*. En caso de no ser atendida su sugerencia por favor lea en *www.tirant.net/index.php/empresa/politicas-de-empresa* nuestro Procedimiento de quejas.

Responsabilidad Social Corporativa: http://www.tirant.net/Docs/RSCTirant.pdf

Delitos informáticos (Cybercrimes)

Alemania

Prof. Dr. Martin Paul Wassmer[1]
Universidad de Colonia

Ya hace más de 30 años se han decretado en Alemania prescripciones penales para la lucha contra la delincuencia informática, que desde ese entonces se han modificado y han sido completadas para considerar el desarrollo tecnológico, así como para poder llevar a cabo las obligaciones legales europeas y de derecho internacional. Las prescripciones penales que existen actualmente protegen primordialmente contra las formas esenciales de la criminalidad cibernética. La importancia de esto, lo muestra un estudio actual de la empresa consultora KPMG AG. Según este estudio, en Alemania estuvieron afectados por criminalidad cibernética en los años 2012 y 2013, 27 % de las empresas y en los años 2014 y 2015 esta cifra ya habría aumentado a un 40%[2].

I. Definición de los ciberdelitos

Para la "delincuencia o criminalidad cibernética" no existe hasta el momento **una definición general válida.** Bajo éste término, se entienden todos los hechos penales que han sido consumados a través del aprovechamiento de las técnicas de información y comunicación o contra ellas. Común es una distinción entre la"**delincuencia de Internet"** y **"delincuencia informática o por medio de un ordenador"**, es decir, hechos penales, en los cuales el Internet o respectivamente un ordenador es el medio (Tatmittel) u objeto del hecho (Tatobjekt)[3]. Si bien, esta circunscripción no es lo suficientemente precisa, ya que las áreas se interfieren entre si considerablemente, la estadística criminal policial de la Oficina Federal de Investigación Criminal (Bundeskriminalamt) se apoya, sin embargo en tal diferencia, cuando se trata de describir los medios de hecho; de este modo presenta como medio de hecho el **"medio de hecho Internet"** y como forma de delincuencia especial la **"delincuencia informática o por medio de un ordenador"**. De una manera parecida distingue también el "Bundeslagebild Cybercrime", elaborado anualmente y dirigido así mismo por la Oficina Federal de Investigación Criminal, entre hechos penales que van contra el Internet, las redes de datos, los sistemas técnicos de información o sus datos **(Cybercrime en sentido específico)** y hechos penales que son cometidos mediante esta técnica de información **(Cybercrime en sentido general)**[4]**.**

II. Significado práctico

1. Criminalidad informática o mediante un ordenador

Según la estadística criminal policial, se registraron en el 2015 en el área de la **"criminalidad informática" 70.068** casos; esto significa una disminución de un 5,2% frente al año pasado. Sin embargo, este retroceso se debe por sobre todo a un cambio del registro estadístico[5]. Dado que desde el 2014 son registrados exclusivamente hechos penales, en los cuales se encuentren puntos de referencia concretos para una **conducta tipificada (Tathandlung) dentro de Alemania**[6]. La consecuencia fue que, si bien —mirado del punto político criminal, esto no dejaba de ser anhelado— los números de estos casos disminuyeron, sin embargo, la dimensión de la delincuencia no fue reflejada. Ya que, precisamente para la criminalidad informática o por medio de un ordenador, el lugar de comisión del delito no tiene un significado primordial. Entretanto se ha generado eso si, un cambio en el punto de vista en otro sentido: a partir del 2017 deben ser nuevamente incluidos, también aquellos delitos que han sido consumados en el extranjero o en algún lugar desconocido[7]. Por lo demás, no son considerados también hechos penales, los cuales estén motivados ya sea políticamente o de índole noti-

ciera[8]. La **cuota de esclarecimiento** en la delincuencia informática o mediante un ordenador, hacía en 2015 un 33,8% y estaba todavía por debajo del promedio (hechos penales en total, sin contar los hechos extranjeros: 53,4%[9]) que no es sorprendente, teniendo en cuenta lo global y el anonimato del Internet.

La "Bundeslagebild Cybercrime" capta con el **Cybercrime en sentido específico**, el área más importante de la "criminalidad informática". En el año 2015 se registraron un total de **45.793 casos[10]**. De ellos, se registraron 23.562 casos de **estafa informática (§263a StGB)**. El engaño con autorizaciones de acceso para servicios de comunicación, que representa igualmente una estafa informática, registró 1.878 casos, con lo que este delito es así, responsable para más de la mitad de todos los hechos penales (55,5%) registrados. Los hechos penales restantes tuvieron una menor participación: espionaje e intercepción de datos junto a acciones de preparación (§§202a, 202b 202c StGB): 21,0%; falsificación de datos considerables y engaño en el tráfico jurídico por medio de procesamiento de datos (§§269, 270 StGB): 15,7%; cambio de datos y sabotaje informático (§§303a, 303b StGB): 7,7%. **La suma total de los daños fueron de 40,5 millones de euros**. Sin embargo, fueron registrados solo daños en relación a la estafa informática, de manera que no es posible hacer declaraciones susceptibles acerca de la totalidad de los daños real[11].

Toda el área de la "criminalidad informática" abarca además **la estafa (§263 StGB)** mediante tarjetas de débitos con PIN obtenidas ilegalmente; este delito se registró al menos en 23.790 casos, y la **piratería de software (§§106 ss. UrhG),** la cual es muy inferior con un numero de hechos registrados por la policía de solo 485 casos[12].

2. El Internet como medio de hecho

Bajo la clave especial "Internet como medio de hecho"[13] comprende la estadística criminal policial, todos los hechos penales que son consumados bajo la utilización del Internet. Estos hechos penales pueden concernir casi todas las áreas de delito. En el año 2015 fueron registrados en total 244.528 casos, lo que significa un descenso de 1,0% frente al año pasado. Con ello, esta forma de comisión a todos los hechos penales (sin faltas legales extranjeras) cubrió sólo un 4,1%, es decir, la mayoría de los hechos penales siguen siendo consumados en modo "offline" ósea "desconectado". Principalmente se trató de **delitos de estafa** (§§263 ss. StGB; 182.278 casos; parte: 74,5%), entre ellos sobre todo la estafa de mercancías y estafa de crédito de mercancías (123.034 casos; 67,5%). Otras partes considerables tenían junto a la **criminalidad informática** (cf. anteriormente bajo II.1.) **delitos de injuria** (§§185 ss. StGB; 11.891 casos; 4,9%), la **difusión de documentos pornográficos** (§§184 ss. StGB; 6.983 casos; 2,9%) y **hechos penales en relación a los derechos de autor** (p. ej., §§106 ss. UrhG; 3725 casos; 1,5%).

3. Cifra clara y oscura

Se debe tener en cuenta que precisamente en la criminalidad cibernética, según lo señalan muchos estudios, existe un **campo oscuro muy amplio** [14]. Por este motivo, las estadísticas demuestran sólo un pequeño fragmento de la dimensión real de la criminalidad cibernética. **Las causas** de ello, están en que numerosos hechos penales no sobrepasan la fase de tentativa o simplemente no son observados debido a las precauciones mejoradas de protección técnica, en que además a menudo no se produce ningún daño y si se produce, muchos perjudicados sobre todo empresas, no denuncian estos hechos penales para no perder su reputación de "compañero seguro y fiable"[15].

III. Delitos cibernéticos en sentido específico

De interés especial son los hechos penales de **delitos cibernéticos en sentido específico**, dado que en ellos el procesamiento de datos es primordial para la perpetración del hecho, con lo que de esta manera ellos forman el "núcleo" de la criminalidad cibernética. Los hechos penales se encuentran en las **diferentes secciones** del StGB, ya que hechos penales tradicionales (estafa; falsificación de documentos; violación al secreto de la palabra y el secreto de carta; daño material) son complementados en los casos de la "ejecución digital".

1. Estafa informática (§263a StGB)

El §263a StGB se introdujo ya por la segunda Ley contra la lucha de la delincuencia económica **(2. WiKG)** del 15.05.1986[16] entrando en vigor el 01.08.1986, con el fin de cerrar lagunas penales, ya que el tipo **penal de estafa** (§263 StGB) no puede concebir procesamiento de datos, dado que falta la característica del engaño, el error y la orden de disposición de bienes, de una persona[17]. La **Ley 35 de modificación de Derecho Penal[18]** agregó el 28.12.2003 en la conversión de la resolución marco de la UE 2001/413 /JI en la lucha contra la estafa y falsificación en relación a medios de pago no mone-

tarios[19], el párrafo 3 y 4 para amenazar independientemente con pena **acciones de preparación[20]**.

a. La figura delictiva (Grundtatbestand) de la estafa informática (§263a párrafo 1 StGB), está transcrita de la estafa y según la opinión dominante (h.M.)[21] debe ser rigurosamente interpretada a base de ésta **(interpretación específica de estafa / betrugsspezifische Auslegung)**. Ella contiene **cuatro alternativas de hecho**. Con pena privativa de libertad de hasta cinco años o con multa será castigado, quién con el propósito de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, a través de una estructuración incorrecta del programa **(1. alternativa, manipulación de programa)**, por la utilización de datos incorrectos o incompletos **(2. alternativa, manipulación input)**, por el empleo no autorizado de datos **(3. alternativa, abuso de datos informáticos)** o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso **(4. alternativa, figura delictiva recaudatoria** para agrupar otros hechos y manipulaciones técnicas).

Para el registro de la criminalidad cibernética tiene § 263a StGB un significado sobresaliente (cf. bajo II.1.). En la práctica dominan el uso ilícito de **tarjetas bancarias robadas o falsificadas** y tarjetas de crédito en cajeros automáticos y terminales de cajas[22]. Más allá se trata de casos en los cuales, autores se han conseguido reconocimientos de utilidad como PINs, TANs u otras llaves de acceso a través de **"Phishing**" (por Mail/ SMS/mensaje instantáneo) o **"Pharming"** (desviando al autorizado a páginas falsificadas) y emplean éstos luego en Online-Banking[23]. También son concebidas "la estafa con autorizaciones de acceso para servicios de comunicación", especialmente el "**Phreaking",** en el cual líneas telefónicas y respectivamente direcciones de datos son usadas a cuenta de propietarios de enlaces ajenos, como también las **"tarjetas pirata"** para la descodificación de Pay-TV y la utilización ilegal de WLANs con clave[24].

A causa de la remisión del §263a párrafo 2 StGB a la estafa, es la estafa informática o mediante un ordenador, una falta, que no sólo percibe una **tentativa** punible, sino en la que los **casos especiales agravantes** del §263 párrafo 3 StGB son aplicables, para los cuales esta prevista una pena aumentada, o sea, una pena privativa de libertad de seis meses hasta diez años. Además, en los casos de **comisión perteneciendo a una banda o comisión profesional** se aplica el §263 párrafo 5 StGB, que está amenazado con pena privativa de libertad de un año hasta diez años y representa por ende un crimen.

b. §263a párrafo 3 StGB debe penalizar **acciones de preparación especialmente peligrosas**. Con pena privativa de libertad de hasta tres años o multa es castigado, quien produce y crea programas informáticos, se consigue así mismo o a un tercero, lo pone en venta, lo guarda o se lo deja a otra persona, cuyo objetivo es la comisión de un hecho penal según el §263a párrafo 1 StGB. Debido al momento prematuro de consumación del delito, dispone §263a párrafo 4 StGB el empleo correspondiente de los arreglos del §149 párrafo 2 y 3 StGB que regulan al arrepentimiento activo. Según esta Ley, el programa **"no tiene que estar determinado exclusivamente"** para la comisión de una estafa informática o mediante un ordenador[25]. Este punto de vista es extremadamente problemático, dado que muchos programas pueden ser utilizados no sólo con objetivos legales, sino también con objetivos ilegales **(los así llamados, Dual-Use-Tools)**. Por eso, se exige restrictivamente que el programa "principalmente"[26] sirva a la consumación de un hecho penal según el §263 párrafo 1 StGB y que respectivamente éste tendría que ser el objetivo "primordial"[27] de tal programa. Con vista a la jurisdicción del Tribunal Constitucional Federal (BVerfG)[28] hacia el §202c StGB, se debería contrariamente incluso exigir que el programa haya sido desarrollado o modificado con la **intención** de ser empleado en la comisión de hechos penales y que tal intención se haya **manifestado objetivamente** (p. ej. mediante publicidad en Internet)[29].

2. Piratería informática e intercepción de datos con acciones de preparación (§§202a, 202b 202c StGB)

El §202a StGB fue incorporado igualmente por el **2. WiKG** en 1986 para cerrar lagunas penales en el área de la violación de la intimidad y del secreto personal[30]. A través de la **Ley 41 de modificación del Derecho Penal**[31] y en la conversión de la convención de Cybercrime del Consejo de Europa del 08.11.2001[32] y de la Resolución marco de la UE en 2005/222 /JI del 24.02.2005 sobre ataques a sistemas de información[33], se amplió con fecha 11.08.2007 la figura delictiva para la lucha contra nuevos fenómenos de delincuencia. Al mismo tiempo se incorporaron el §202b StGB y §202c StGB. En la práctica, se conciben de todos estos hechos penales, sobre todo el **"robo"** de identidades digitales, datos de tarjetas de crédito, datos de E-Commerce o datos de cuenta, especialmente por Phishing y Pharming. Luego los datos robados son por lo general vendidos en "Darknet" o son utilizados por el mismo autor[34].

a. §202a párrafo 1 StGB (piratería informática) castiga con pena privativa de libertad de hasta tres años o con multa a aquél, quien sin autorización se procure para sí o para otro datos que no están determinados para él y que están asegurados especialmente contra su acceso no autorizado, bajo superación de aquella protección. **Datos** en el sentido del párrafo 1 son según el §202 párrafo 2 StGB tales, que están guardados o son transmitidos de una manera electrónica o magnética, ósea de una manera no directamente perceptible. La noción "datos" es muy amplia de entender, bajo este término caen todos los datos que están retenidos en cintas magnéticas, disquetes, discos duros, USB-Sticks, tarjetas de almacén (también en Smartphones), tarjetas de crédito, discos compactos o DVD[35].

Esta figura delictiva está en primer lugar restringida por el requisito de la **protección especial**, dado que esto requiere precauciones que excluyen el acceso a datos o lo dificultan por lo menos no insignificantemente[36]. En segundo lugar la protección especial de acceso tiene que ser **superada,** a lo cual se exige un esfuerzo de tiempo o técnicos de no menor importancia[37]. Por este motivo, p. ej. según la opinión dominante[38] (h.M.) el **Skimming**, ósea el desciframiento de datos contenidos o guardados en una banda magnética de una tarjeta de pago para fabricar duplicados de tarjetas, no cumple básicamente la figura delictiva. Sin embargo, estos casos pueden ser absorbidos bajo el §202c StGB (cf. abajo III.2.c.), si es que se utilizan programas informáticos[39]. Una tercera restricción provoca la noción **"sin autorización"** que debe garantizar que, p. ej., la localización de lagunas de seguridad en el sistema de informática de una empresa, no sean percibidas, en el caso que un "Hacker" haya sido encomendado por la empresa con cuya tarea[40].

b. Según el §**202b StGB (intercepción de datos)** será castigado con pena privativa de libertad de hasta dos años o con multa, quien sin autorización se procure para sí o para otro, bajo el empleo de medios técnicos, datos que no estén determinados para él (§202a párrafo 2) a través de una transmisión de datos no públicos o de la irradiación electromagnética de una instalación informática. Aquí esta percibida cada forma de la **transmisi**ón de datos, de manera que no sólo están incluidas las transmisiones por WLAN sino también, tales por E-Mail, teléfono, Voice over IP o fax. La figura delictiva esta especialmente restringida por la noción **"no público"** para lo que sin embargo, no el tipo o contenido de los datos son determinantes, sino el tipo del proceso de transferencia[41]. De esta manera, también esta comprendida la intercepción por **E-Mails**, e independientemente de una posible codificación[42]. No está percibido p. ej., el Phishing, en el cual la víctima consigna intencionalmente los datos de acceso al autor[43].

c. §202c StGB (p**reparación de espionaje e intercepción de datos)** será castigado con pena privativa de libertad de hasta dos años o con multa, quien prepara un hecho penal según el §202a o §202b StGB, mientras él produzca o cree, se procure para sí o para otro, venda, deje en manos de otro, difunda o haga de cualquier manera accesible, (1) contraseñas u otros códigos de protección que permiten el acceso a datos, o (2) programas informáticos, cuyo objetivo sea la consumación de tal hecho. También aquí son aplicables los arreglos del §149 párrafo 2 y 3 StGB de arrepentimiento activo. El legislador quería percibir con esta prescripción penal por sobre todo **Hacker-Tools**, que en Internet son muy divulgadas y pueden ser cargadas anónimamente[44]. Igualmente aquí existe —como en §263a párrafo 3 StGB— la problemática de que los programas pueden también ser utilizados con objetivos legales (p. ej., como programas de prueba por empresas de seguridad). Por ello, según la jurisdicción del BVerfG (cf. III.1.c.) es necesaria una interpretación muy restrictiva.

3. Falsificación de datos de prueba relevantes y el engaño en el trafico jurídico en la elaboración de datos (§§269, 270 StGB)

El §269 y §270 StGB se incorporaron igualmente ya por el 2. WiKG en 1986 para evitar lagunas penales existentes en los delitos de **falsificación de documentos**, ya que §267 StGB (falsificación de documentos) no interviene si los datos que se han introducido en un ordenador, son modificados de una manera visualmente no perceptible[45].

Según el §269 párrafo **1 StGB (falsificación de datos de prueba relevantes)** será castigado con pena privativa de libertad de hasta cinco años o con multa, quien guarde o modifique datos de prueba relevantes para el engaño en el trafico jurídico, de tal manera que en su percepción existiera un documento falso o adulterado o quien utilice aquellos datos guardados o modificados. Según §270 StGB el engaño en el trafico jurídico y la influencia del procesamiento de datos en el trafico jurídico son equivalentes. Esta cláusula de equiparación debía crear claridad legal para los casos, en los cuales el autor no envía documentos o datos a una persona, sino que los guarde en un ordenador[46]. En la práctica estos hechos penales no sólo perciben los casos, en los cuales personas son engañadas por el envío de E-Mails, bajo **simulación de identidades reales**

o empresas para revelar informaciones de cuenta o de datos de tarjetas de crédito, sino, p. ej. también el envío de **Schadsoftware** (Softwares dañinos) en los E-Mails que están camuflados como facturas[47].

También en estos delitos la **tentativa** es punible (§269 párrafo 2 StGB). Además, no solo existe una pena aumentada para **casos agravantes especiales** (§269 el párrafo 3 StGB), sino también para los casos de contra bandas y consumación profesional, existe un hecho de crimen (§269 párrafo 4 StGB).

4. Alteración de datos y sabotaje informático (§§303a, 303b StGB)

Finalmente, se incorporaron ya por el 2. WiKG el §§303a y 303b StGB para cerrar lagunas penales en el área del **daño material** (§303 StGB)[48]. A través de la Ley 41 de modificación del Derecho Penal (cf. III.2.) las prescripciones penales fueron complementadas con fecha del 11.08.2007 y las acciones de preparación fueron penalizadas. En la práctica, los hechos delictivos perciben muchas formas del "daño material digital", junto a **ataques DoS-/DDos** típicamente también la difusión y empleo de **Schadsoftware** (troyanos, virus, gusanos digitales etc.)[49].

Según el §303a párrafo 1 StGB (alteración de datos) será castigado con pena privativa de libertad de hasta dos años o con multa, quien borre, suprima, inutilice, o cambie datos de una manera antijurídica. Además será castigado según los hechos básicos del §303b párrafo 1 StGB (sabotaje informático) con pena privativa de libertad de hasta tres años o con multa, quien altere un procesamiento de datos, que sean para otra persona de un significado esencial, y que asimismo los perturbe o cambie de una manera considerable, en el que (1) consuma un hecho según el §303a párrafo 1 StGB, (2) introduzca o transfiera datos, con la intención de causar a otra persona una desventaja o (3) destruya, estropee, inutilice, elimine o cambie datos de una instalación informática. Si el procesamiento de datos es para una compañía extranjera, una empresa extranjera o una autoridad administrativa de un significado primordial, la pena de reclusión asciende hasta cinco años o multa según §303a párrafo 2 StGB. También aquí la **tentativa** es punible (§303a párrafo 2 StGB; §303b párrafo 3 StGB) y en todo caso, existe para el sabotaje informático un arreglo para **casos especiales agravantes** (§303b párrafo 4 StGB). Con respecto a la preparación de hechos penales se debe aplicar el §202c StGB correspondientemente (§303a párrafo 3 StGB; §303b párrafo 5 StGB).

IV. Perspectiva general

Las múltiples apariciones de la criminalidad cibernética pueden ser lo suficientemente combatidas en Alemania con el **derecho penal materia**l disponible. Sin embargo, las prescripciones penales podrían estar en parte mejor sistematizadas y estar restringidas más agudamente[50]. Además, en el **derecho procesal** podrían ser creadas nuevas autorizaciones de intervención[51]. Dado que el **potencial de peligro y de daño** asciende constantemente, porque el significado del Internet en el área privada y comercial (medios sociales; comercio en línea; Onlinebanking; "el Internet de las cosas" —p. ej. televisores inteligentes". La industria 4.0"— la dirección basada en Internet de procesos de empresa) aumenta y con eso también crecen las posibilidades de consumar un hecho, de una manipulación y de un ataque[52]. Ha esto se le agrega que por un lado, los **autores** se organizan cada vez más profesionalmente y sin embargo, por otra parte también cada día mas personas sin conocimientos informáticos especiales, tienen la posibilidad de cometer delitos cibernéticos[53]. Asimismo, hoy en día el "Underground Economy" digital pone a disposición un servicio muy amplio (p. ej. software, las plataformas de comunicación, servicios anónimos de Hosting)[54], el cual hace posible y facilita respectivamente la consumación de hechos penales. Finalmente, se puede decir que una lucha efectiva de la criminalidad cibernética como forma de delincuencia transnacional requiere la **cooperación** de las autoridades de seguridad y de las empresas económicas, no sólo a nivel nacional, sino también a nivel europeo e internacional. Con este objetivo, se creo en Alemania ya en Abril del 2011 el **Centro Nacional de Defensa Cibernética (NCAZ)** como institución de cooperación de zonas de seguridad alemanas para la defensa de ataques electrónicos en las infraestructuras técnicas de información y comunicación[55]. En abril del 2017 el Ministerio de Defensa Federal consagró incluso la base para un **ejército cibernético** y así proteger en el futuro de una mejor manera, las infraestructuras alemanas de ataques de Hacker y de Estados y Potencias extranjeras[56].

Bibliografía general

Cornelius, Besonderheiten des Straf- und Strafprozessrechts, en: Leupold/Glossner (ed.), Münchener Anwaltshandbuch IT-Recht, 3. edición 2013; Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009; Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. edición 2012; Rohrlich, Crime Scene Internet.

Ein Streifzug durch das Computer- und Internetstrafrecht, 2015; Malek/Popp, Strafsachen im Internet, 2. edición 2015; Marberth-Kubicki, Computer- und Internetstrafrecht, 2. edición 2010; Sieber, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, München 2012; Spindler/Schuster (ed.), Recht der elektronischen Medien, 3. edición 2015; Vassilaki/Martens, Computer- und Internetstrafrecht 2003; Wassmer, Computerbetrug (§ 263a StGB), en: Leitner/Rosenau (ed.), Wirtschafts- und Steuerstrafrecht, 2017.

Notas

1 Traducción de Aniza Waleska Izeta López, Santiago de Chile/Colonia.

2 KPMG AG, e-Crime, Computerkriminalität in der deutschen Wirtschaft, 2015, p. 4 (https://home.kpmg.com).

3 Gercke, en: Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, nº marg. 73 con más antecedentes.

4 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 5 (https://www.bka.de).

5 Bundeskriminalamt, Polizeiliche Kriminalstatistik 2015, p. 354 (https://www.bka.de).

6 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 5.

7 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 5, nota 01.

8 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 5.

9 Bundeskriminalamt, Polizeiliche Kriminalstatistik 2015, p. 4.

10 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 6.

11 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 7.

12 Bundeskriminalamt, Polizeiliche Kriminalstatistik 2015, p. 354.

13 Bundeskriminalamt, Polizeiliche Kriminalstatistik 2015, p. 30 s.

14 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 5, 8 con más antecedentes.

15 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 8.

16 BGBl. I p. 721.

17 BT-Drs. 10/318, p. 18; 10/5058, p. 20.

18 35. Strafrechtsänderungsgesetz, BGBl. I 2003 p. 2838.

19 DOUE L 149, p. 1; detallado Wassmer, en Pötz/Grützner/Kreß, (ed.), Internationaler Rechtshilfeverkehr in Strafsachen, 3. edición 2012, III C 4.9.

20 BT-Drucks. 15/1720, p. 10.

21 BGHSt 38, 120, 124; 47, 160, 162 s.; Wassmer, Computerbetrug (§ 263a StGB), en: Leitner/Rosenau (ed.), Wirtschafts- und Steuerstrafrecht, 2017, nº marg. 37 ss. con más antecedentes.

22 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 6.

23 Wassmer, Computerbetrug (§ 263a StGB), en: Leitner/Rosenau (ed.), Wirtschafts- und Steuerstrafrecht, 2017, nº marg. 54 con más antecedentes.

24 Wassmer, Computerbetrug (§ 263a StGB), en: Leitner/Rosenau (ed.), Wirtschafts- und Steuerstrafrecht, 2017, nº marg. 56 s. con más antecedentes.

25 BT-Drucks. 15/1720, p. 11.

26 Heger, en: Lackner/Kühl (ed.), StGB, 28. edición 2014, § 263a nº marg. 26b.

27 Fischer, StGB, 64. edición 2017, nº marg. 31.

28 BVerfG CR 2009, 673.

29 Wassmer, Computerbetrug (§ 263a StGB), en: Leitner/Rosenau (ed.), Wirtschafts- und Steuerstrafrecht, 2017, nº marg. 107 con más antecedentes.

30 BT-Drs. 10/5085, p. 28.

31 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität, BGBl. I 2007 p. 1786.

32 ETS-No. 185.

33 DOUE L 69, p. 67.

34 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 6.

35 Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. edición 2012, nº marg 538.

36 BT-Drs. 16/3656, p. 10.

37 BT-Drs. 16/3656, p. 10.

38 BGH NStZ 2011, p. 154.

39 Wassmer, Computerbetrug (§ 263a StGB), en: Leitner/Rosenau (ed.), Wirtschafts- und Steuerstrafrecht, 2017, nº marg. 108 con más antecedentes.

40 BT-Drs. 16/3656, p. 10.

41 BT-Drs. 16/3656, p. 11.

42 Eisele, en: Schönke/Schröder, StGB, 29. edición 2014, nº marg. 4a.

43 Eisele, en: Schönke/Schröder, StGB, 29. edición 2014, nº marg. 4.

44 BT-Drs. 16/3656, p. 12.

45 BT-Drs. 10/318, p. 31.

46 BT-Drs. 10/318, p. 34.

47 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 6.

48 BT-Drs. 10/5058, p. 34.

49 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 6.

50 Sieber, en: 69. Deutscher Juristentag München 2012, Thesen der Gutachter und Referenten, p. 32 s. (www.djt.de).

51 Recomendaciones Sieber, en: 69. Deutscher Juristentag München 2012, Thesen der Gutachter und Referenten, p. 34.

52 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 19.

53 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 19

54 Bundeskriminalamt, Bundeslagebild Cybercrime 2015, p. 11.

55 https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, 2011, p. 8 s.

56 http://www.zeit.de/digital/internet/2017-04/cyber-armee-bundeswehr-ursula-von-der-leyen; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, 2016, p. 38 s.

Argentina

Luis Fernando Niño (UBA)[1]

(*Leyes nº. 26.388, 26.685 y 26.904*)

I. La necesidad de protección de bienes intangibles ante la comisión de conductas perjudiciales concretadas a través del empleo de medios informáticos o tecnologías digitales interesó vivamente a la comunidad jurídica argentina.

A partir de 1996 se sucedieron numerosas iniciativas parlamentarias destinadas a reformar el Código Penal de la Nación, ya mediante una ley integral y concordada, a fin de adaptar cada tipo penal preexistente a esa nueva modalidad comisiva, ya a través de la sanción de una ley complementaria con idéntica finalidad[2].

El último de los proyectos citados en la precedente nota al pie representó una versión depurada de los anteriores y condujo a la sanción de la actual ley 26.388 (B.O. 25/6/2008); mas, al optar por la mera modificación de los tipos penales tradicionales, la nueva normativa alcanzó un número muy limitado y especifico de figuras del Código en vigor, a saber: 1) ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (*Artículo 128 del C.P.*), 2) violación de correspondencia electrónica (*Artículo 153 del C.P.),* 3) acceso ilegítimo a un sistema informático (*Artículo 153 bis del C.P.*), 4) publicación abusiva de correspondencia (*Artículo 155 del C.P.*), 5) revelación de secretos (*Artículo 157 del C.P.*), 6) delitos relacionados con la protección de datos personales (*Artículo 157 bis del C.P.*), 7) defraudación informática (*Artículo 173, inciso 16, C.P.*), 8) daño informático (*artículo 183 y 184, C.P.*), 9) interrupción o entorpecimiento de las comunicaciones (*Artículo 197 C.P.*), 10) alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (*Artículo 255 del C.P.*).

A tales variaciones en la Parte Especial se sumaron las modificaciones terminológicas incorporadas en el artículo 77 de dicho código de fondo por la misma ley, complementadas ulteriormente por la introducida mediante la ley 26733 (B.O. 28/12/11)[3]. Tal como destaca Marcelo A. Riquert, *"la ley 26.388 ha significado un sustancial avance sobre temas cuya consideración venía siendo reclamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias".*[4]. Por lo pronto, mediante tal instrumento legal, Argentina cumplimentó los requerimientos formulados en el nivel internacional por el Convenio de Ciber-criminalidad suscrito en Budapest en 2001[5].

Vale poner de relieve que el legislador argentino se abstuvo de introducir tipologías de sujetos activos en los preceptos incorporados al texto sustantivo, tales como los definidos mediante los anglicismos "*hacker", "cracker", "preaker"* o *"phreaker", "phisher", "sniffer", "virucker", "ciberbullyng*", o bien las locuciones sustantivas "propagandista informático", "pirata informático", o "ciber-acosador". Es ponderable, asimismo, la prudencia con que se confeccionaron los distintos tipos legales, todos ellos de carácter doloso salvo la modalidad culposa del depositario, en el caso de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (artículo 255, 2º párrafo, del C.P.), y ninguno omisivo.

Hasta el momento de redacción de este informe, completa el panorama jurídico-penal argentino referido al tema la ley 26.904 (B.O. 11/12/13), que introdujo en el Código Penal de la Nación la figura del "*grooming*" o ciber-acoso sexual a menores, a través de la nueva redacción del artículo 131, que establece: "*Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*".

Refiere Hugo Vaninetti que el "*grooming*" "*engloba básicamente la realización de actos preparatorios a través de las modernas tecnologías de la comunicación e información para perpetrar posteriormente delitos contra la integridad sexual. Importaría decir que es una etapa virtual previa al abuso sexual en el mundo real*"[6].

II. Es inocultable que diversos comportamientos pasibles de comisión a través de dispositivos digitales permanecen faltos de la debida descripción y punición en el ordenamiento penal sustantivo argentino. El Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación de 2014, debido a la Comisión creada por decreto del Poder Ejecutivo Nacional nº 678/2012, incorporaba otras figuras, tales como la responsabilidad penal de las empresas prestatarias de servicios de internet, pero la absurda falta de tratamiento parlamentario de dicho ordenamiento, debido a infundios políticos de baja ralea, ha impedido hasta el momento contar con ese catálogo actualizado y armónico de normas penales, incluyendo las alusivas a la criminalidad informática.

Entretanto, parte de la doctrina penal argentina, sin renunciar a una política criminal reductora del poder punitivo, ha sugerido la incorporación de tipos legales,

sea como añadidos a los tradicionales, o como figuras especiales en el marco de algunas de las abundantes leyes complementarias del Código Penal. Es el caso de Carlos Christian Sueiro[7], quien propone adicionar preceptos referidos a ese específico universo a los tipos preexistentes de hurto (*Artículo 162 del C.P.*)[8], de revelación de secretos de Estado y ultraje a los símbolos patrios (*Art. 222 del C.P.*)[9], de incendios y otros estragos (*Artículo 186 del C.P.*)[10], de falsificación de documento público y privado (*Artículo 292 del C.P.*) y de uso de documento falso o adulterado (*Artículo 296 del C.P*)[11], así como incluir modalidades comisivas de tal índole en los regímenes penales tributario (*leyes 24.769 y 26.735*), cambiario (*leyes 19.359, 22.338, 23.928 y 24.144 y decreto 480/95*), y aduanero *(ley 22.415)*[12].

Marcelo A. Riquert y Pablo A. Palazzi alertan, de igual manera, acerca de la escasa exhaustividad en el tratamiento de la materia en análisis al sancionarse las reformas de las leyes 26.388 y 26.904. Mencionan en tal dirección los casos de la llamada ciber-ocupación o registro impropio de nombres de dominio[13], el "*Spamming"* o "correo basura" o publicidad no solicitada[14]; la captación ilegal y difusión de datos, imágenes y sonidos[15], la simple posesión de material pornográfico infantil y la responsabilidad de los proveedores[16].

Otros publicistas argentinos, como Gustavo E. Aboso, Fernando Machado Pelloni y Nora Chervñasky, se suman a los tres ya mencionados en punto a proponer figuras que no se encuentran acogidos por nuestro ordenamiento, a diferencia de otros sistemas jurídicos, como los de Alemania, España, Estados Unidos de Norteamérica, y Reino Unido de Gran Bretaña e Irlanda del Norte.

Se trata de los llamados "c*iberbullying"* (ciberacoso)[17], "*ciberStalking"* (ciber-hostigamiento)[18], sustitución de identidad[19], ciber-odio[20] y responsabilidad penal de las empresas prestadoras del servicio de internet[21].

otro rasgo deficitario de la legislación argentina, de cara a la problemática que nos convoca, está configurado por la falta de reformas a nivel procesal penal que incluyan referencias a temas tales como la prueba electrónica o evidencia digital, pese a ser un requisito incluido en el recordado convenio de cibercriminalidad de Budapest De 2001. Así lo advierten autores como Daniel Petrone[22], Marcos Salt[23] y Carlos Christian Sueiro[24]. Ni siquiera el más reciente Código Procesal Penal de la nación (Ley 27063) sancionado a fines del año 2014, mas suspendido en su vigencia por un mero decreto del poder ejecutivo, cuenta con un capítulo destinado a la regulación de la prueba digital[25].

en menester, en consecuencia, una legislación procesal penal en materia de criminalidad informática que prevea, cuando menos, la conservación rápida de datos informáticos almacenados, la conservación y revelación parcial rápidas de los datos relativos al tráfico, la orden de presentación, el registro y confiscación de datos informáticos almacenados, la obtención en tiempo real de datos relativos al tráfico (art. 20 del *convenio)* y la interceptación de datos relativos al contenido, como lo prevén los artículos 16 a 21, respectivamente, del convenio de Budapest oportunamente señalado, si se desea lograr la incoporación de la argentina a dicho acuerdo internacional.

Decisiones institucionales recientes, tales como la implementación de dispositivos de vigilancia electrónica de imputados y condenados, tanto a nivel de la justicia nacional como de la ciudad autónoma de buenos aires[26], así como la posible incorporación de medios electrónicos entre las técnicas de investigación criminal, tornan más imperiosa aun la actividad parlamentaria que subsane la demora en abarcar normativamente esas y otras situaciones vinculadas al empleo del creciente arsenal cibernético.

Bibliografía

Aa.vv. - Dupuy Daniela (Dirección) – Kiefer Mariana (Coordinación)
"Cibercrimen. Aspectos De Derecho Penal Y Procesal Penal.
Cooperación Internacional. Recolección De Evidencia Digital.
Responsabilidad De Los Proveedores De Servicios De Internet"., Prólogo Germán C. Garavano, Presentación: Luis J. Cevasco, 1ª Edición, Editorial Bdef, Buenos Aires - Montevideo, 2017.

Aa.vv. - Riquert Marcelo A. (Coordinador) "Ciberdelitos", 1ª Edición, Editorial Hammurabi, Buenos Aires, 2015.

Aboso Gustavo Eduardo. "Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación"., Prólogo de Mirentxu Corcoy Bidasolo,1ª Edición, Editorial BdeF, Buenos Aires - Montevideo, 2017.

Aboso Gustavo Eduardo – Zapata María Florencia. *"Cibercriminalidad y Derecho Penal"*., Editorial BdeF, Buenos Aires, 2006.

Assange Julian. *"Criptopunks. La libertad y el futuro de internet"*., 1ª Edición, Editorial, Marea Editorial, Buenos Aires, 2013.

Balardini Sergio. "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la Web 2.0. El caso de Facebook", publicado en la obra de Barindelli Florencia –Gregorio CarloS G. (Compiladores), "Datos personales y libertad de expresión en las redes sociales digitales. Memorándum de Montevideo", Editorial Ad-Hoc, Buenos Aires, 2010.

Bauman Zygmunt & Lyon David. *"Vigilancia líquida"*, título original en inglés: *Liquid Surveillance*, 1ª Edición, Editorial Paidós, Buenos Aires, 2013.

Candarle Gisela. *"Hacia la justicia digital en la Ciudad de Buenos Aires"*, publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com, Editorial Albremática - El Dial, Biblioteca Jurídica *on line*, el 10 de agosto de 2011. (elDial.com DC167D).

Carnevale Carlos A. *"¿El acceso a internet es un Derecho Humano?",* publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com. 2011, 9 de Noviembre de 2011, elDial.com - DC1746.

Cassin Barbara. *"Googléame. La segunda misión de los Estados Unidos"*, 1ª Edición, Editorial, Fondo de Cultura Económica, Buenos Aires, 2008.

Cherñavsky Nora A. *"Responsabilidad penal de los proveedores de servicios de internet".,* publicado en la *Revista Informática y Delito.*

Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP), Grupo Nacional, Facultad de Derecho, UBA, Marzo de 2014, Buenos Aires, 2014, pp. 17/32, ISBN 978-987-3720-08-6.

Domscheit-Berg Daniel. *"Dentro de WikiLeaks. Mi etapa en la Web más peligrosa del mundo"*, Título original: *"Inside WikiLeaks"*, Traducción: Ana Duque de Vega y Carles Andreu Saburit, 1ª Edición, Editorial Rocaeditorial, Buenos Aires, 2011.

Doueihi Milad. *"La gran conversión digital"*, Titulo original: *"La Grande Conversion numérique"*, Traducción: Julia Bucci, Editorial Fondo de Cultura Económica, Buenos Aires, 2010.

Fillia Leonardo César – Monteleone Romina – Nager Horacio Santiago – Sueiro Carlos Christian.

"Análisis integrado de la Criminalidad Informática", Prólogo Carlos Alberto Elbert, Editorial Fabián J. Di Plácido, Buenos Aires, 2007.

Fillia Leonardo César – Monteleone Romina – Nager Horacio Santiago – Rosende Eduardo E. – Sueiro Carlos Christian.

"Análisis a la reforma en materia de Criminalidad Informática al Código Penal de la Nación (ley 26.388)", Artículo publicado en el Suplemento de Derecho Penal y Procesal Penal de Editorial La Ley, publicado el Jueves, 28 de agosto de 2008, P. 15/41.

Gini Santiago Luis. *"Resolución 654/2009, Nombres de Dominio Locales, Registro Abusivo de Nombres de Dominio y Ciberocupación".*, Publicado en el Suplemento de Alta Tecnología de el Dial.com, Editorial Albremática – El Dial, Biblioteca Jurídica *on line*, Publicado el 14 de abril de 2010, (el.Dial.com DC 1300).

Granero Horacio R. *"El expediente electrónico, próximo a ser Ley Nacional".,* publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com. 2011, elDial.com - CC2684.

Granero Horacio R. *"La sanción de la Ley 26.685 de Expedientes Digitales.*

El principio de equivalencia funcional y la firma digital". publicado en el Suplemento de Derecho de Alta Tecnología de el Dial.com. 2011, elDial.com - CC2736.

Granero Horacio R. *"La inteligencia artificial en la etapa procesal de la prueba"*, publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com. 2012, elDial.com - CC2F45.

Guitiérrez Francés Mariluz. "Reflexiones sobre la ciberdelincuencia hoy (En torno a la Ley penal en el espacio virtual)", Publicado por la Universidad de la Rioja, Redur 3 /Año 2005, P. 70/92.

Ivoskus Daniel. "Obsesión dígital. Usos y abusos en la red", Editorial Grupo Editorial Norma, Buenos Aires, 2010.

Kaplan Carlos. *"Privacidad de ubicación geográfica. Su tratamiento como dato personal sensible"* publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com. 2011, 14 de diciembre de 2011, elDial.com DC178D.

Lanier Jaron. *"No somos computadoras: Un manifiesto".*, Título original en inglés *"You Are Not a Gadget"*, Traducido por Ignacio Gómez Calvo, 1ª Edición, Editorial Debate, Buenos Aires, 2012.

Lo Giudice Maria Eugenia. *"Con motivo de la sanción de la ley que introduce el "delito de grooming" en el Código Penal (año 2013)"*, publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com. 2013, el Dial.com —11-12-2013—DC1C0B.

Molina Quiroga Eduardo – Altmark Daniel Ricardo. *"Tratado de Derecho Informático"*, 1ª Edición, Editorial La Ley, Buenos Aires, 2012.

Morduchowicz Roxana. *"Los adolescentes y las redes sociales. La construcción de la identidad juvenil en Internet".*, Editorial Fondo de Cultura Económica, Buenos Aires, 2012.

Morduchowicz Roxana. *"Los adolescentes del siglo XXI. Los consumos culturales en un mundo de pan-*

tallas", Editorial Fondo de Cultura Económica, Buenos Aires, 2013.

O´Donnell Santiago. "*ArgenLeaks. Los cables de Wikileaks sobre la Argentina, de la A a la Z"*, 4ª Edición, Editorial Sudamericana, Buenos Aires, 2011.

Palazzi Pablo A. "Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388", Editorial Abeledo Perrot, Buenos Aires, 2009.

Palazzi Pablo A. *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, 2ª Edición, Editorial Abeledo Perrot, Buenos Aires, 2012.

Petrone Daniel. *"Prueba Informática"*, Prólogo de Fernando Díaz Cantón, 1ª Edición, Editorial Ediciones Didot, Buenos Aires 2014.

Reggiani Carlos. "Delitos Informáticos", Editorial La Ley, Buenos Aires, 2008 - D, P. 1090.

Riquert Marcelo Alfredo. "Informática y Derecho Penal Argentino", Editorial Ad- Hoc, Buenos Aires, 1999.

Riquert Marcelo A. "delincuencia informática en Argentina y el MERCOSUR", Prólogo de David Baigún, Editorial Ediar, Buenos Aires, 2009.

Sáenz Ricardo – Ruiz Maximiliano. *"Hacia un nuevo modelo de investigación en materia de ciberdelincuencia"*., publicado en el Suplemento de Derecho de Alta Tecnología de elDial.com. 2012, 5 de diciembre de 2012, elDial.com – DC19CB.

Sáez Capel José. *"Informática y Delito"*, 2ª Edición, Editorial Proa XXI, Buenos Aires, 2001.

Sáez Capel José – Velciov Claudia E. *"Comentario al art. 153 bis"*, publicado en AA.VV. "Código Penal comentando", dirigido por David Baigún y Eugenio Raúl Zaffaroni, coordinado por Marco Antonio Terragni, Tomo 5, Editorial Hammurabi, Buenos Aires, 2008.

Salt Marcos G. *"Delitos informáticos de carácter económico"*., en la obra de MAIER JULIO B. J. (Compilador), *"Delitos No Convencionales"*, Editorial, Editores del Puerto, Buenos Aires, 1994, pp. 225/249.

Salt Marcos. *"La relación entre persecución de los delitos informáticos y el Derecho Penal Internacional. Delitos Informáticos aspectos de Derecho Penal Internacional"*., Publicado en la *Revista Informática y Delito. Reunión Preparatoria del Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP)*, Grupo Nacional, Facultad de Derecho, UBA, Marzo de 2014, Buenos Aires, 2014, pp. 237/245, ISBN 978-987-3720-08-6.

Sibilia Paula. "El hombre postorgánico. Cuerpo, subjetividad y tecnologías digitales", 2ª Edición, Editorial Fondo de Cultura Económica, Buenos Aires, 2009.

Sibilia Paula. *"¿Redes o Paredes? La escuela en tiempos de dispersión"*., Editorial Tinta Fresca, Buenos Aires, 2012.

Sueiro Carlos Christian. *"La eficiencia de la reforma en materia de criminalidad informática",* Ponencia presentada y galardonada con el Segundo lugar en el XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal, Facultad de Derecho de la Universidad Nacional de Rosario, Provincia de Santa Fé, 1, 2 y 3 de junio de 2011, Artículo publicado en el Suplemento de Penal y Procesal Penal de Editorial La Ley, Buenos Aires, 2011, pp. 11/22.

Sueiro Carlos Christian. *"La criminalidad informática en el Anteproyecto de Código Penal de la Nación"*., Publicado en la Revista de Derecho Penal de Infojus, Año III, nº 7, Editorial Infojus, Buenos Aires, 2014, pp. 189/233, ISSN 2250-7558.

Sueiro Carlos Christian. *"La criminalidad informática en el Proyecto de Ley de Reforma, Actualización e Integración al Código Penal de la Nación"*., Conferencia presentada en el panel dedicado a parte especial de la Jornada Preparatoria del XIX Congreso Internacional de la AIDP, sobre la *"Sociedad de la Información y Derecho Penal"*, el miércoles 12 de marzo de 2014; Publicado en la Revista de Derecho Penal y Criminología, Año IV, nº 6, Julio 2014, Editorial La Ley, Buenos Aires, 2014, pp. 10/37, ISSN: 0034-7914.

Sueiro Carlos Christian. *"La enseñanza del Derecho Penal en la era de la revolución digital",* Publicado en la Revista de Derecho Penal y Criminología, Año V, nº 2, Marzo 2015, Editorial La Ley, Buenos Aires, 2015, pp. 221/242, ISSN: 0034-7914.

Sueiro Carlos Christian. *"La prueba digital en la criminalidad informática. A propósito del nuevo Código Procesal Penal".* Publicado en la obra de Ángela E. Ledesma (Directora), Mauro Lopardo (Coordiandor), *"El debido proceso penal nº 1",* Editorial Hammurabi, Buenos Aires, 2015, pp. 113/138.

Sueiro Carlos Christian. *"Criminalidad Informática. La eficacia político-criminal de la reforma al Código Penal en materia de delitos informáticos. Análisis de las leyes 26.388, 26.685 y 26.904"*., Prólogo de Marcelo A. Riquert, Editorial Ad-Hoc, Buenos Aires, 2015.

Sueiro Carlos Christian. *"La Pena en la era digital. - A propósito de la introducción de la vigilancia electrónica en el nuevo Código Procesal Penal de la Nación (Ley 27.063)",* Editorial: LA LEY. Revista de Derecho Penal y Criminología, Año VI, nº 4, Mayo 2016, pp.159/170, ISSN nº: 0034-7914.

Sueiro Carlos Christian. *"La pena en la era digital – A propósito del futuro de la pena privativa de la liber-*

tad en la sociedad de la información", Editorial: Fabián J. Di Placido, Revista de Ejecución de la pena privativa de la libertad y el encierro, Año 10, nº 8, 2016, pp. 207/232, ISSN nº 1850-1338.

Sueiro Carlos Christian. *"Criminalidad Informática. La eficacia político-criminal de la reforma al Código Penal en materia de delitos informáticos. Análisis de las leyes 26.388, 26.685 y 26.904",* 1ª Edición, 1ª Reimpresión, Prólogo de Marcelo A. Riquert, Editorial Ad-Hoc, Buenos Aires, 2016.

Sueiro Carlos Christian. *"La Vigilancia Electrónica como forma de morigeración de la prisión preventiva. Alternativas a la prisión en la era digital".,* Revista de Derecho Procesal Penal, *"Alternativas a la prisión. Arresto Domiciliario. Interés Superior del Niño*", Año 2016 – 2, Editorial Rubinzal Culzoni, Santa Fé, 2017, pp. 105/156. ISBN nº 978-987-30-0750-7.

Tazza Alejandro O. *"El delito de Grooming",* publicado en el Dirario La Ley, del viernes 7 de marzo de 2014, Año LXXVIII, nº 45, Tomo La Ley 2014-B, p. 1/3, cita *on line* AR/DOC/32/2014.

Teijeiro Nicolás. *"La protección constitucional de la intimidad en internet con especial referencia a redes sociales",* Publicado en el Suplemento de Alta Tecnología de elDial.com, el 8 de junio de 2011, DC15EF.

Tobares Catalá Gabriel H. – Castro Argüello Maximiliano J. *"Delitos Informáticos"*, Prólogo de Marcelo J. Sayago, Editorial Advocatus, Córdoba 2010.

Tomeo Fernando. *"Responsabilidad penal de los administradores de sitios Web. El caso Taringa!"*, Editorial La Ley, Buenos Aires, 1 de junio de 2011.

Vaninetti Hugo A. *"Media sanción del Senado al Proyecto de "Grooming"*, Publicado en el Suplemento de Actualidad de la Ley, Editorial La Ley, Buenos Aires, 26/04/2012. 1.

Vaninetti Hugo A. *"Inclusión del "Grooming" en el Código Penal",* Publicado en La Ley 16/12/2013, Editorial La Ley, Buenos Aires 2013, AR/DOC/4628/2013

Velazco San Martín Cristo. *"Aspectos jurisdiccionales de la computación de la nube"*, Publicado en el Suplemento de Alta Tecnología de elDial.com el 14 de abril de 2010, elDial.com DC1304.

Notas

1 Para la redacción de este informe ha sido fundamental la aportación del Profesor Christian SUEIRO (UBA), quien prepara su tesis doctoral sobre el mismo tema

2 La nómina de las primeras iniciativas parlamentarias sobre el tópico, con mención del respectivo legislador o ente público auspiciante y del año de su presentación, es la siguiente: 1) Leonor Esther Tolomeo (1996); 2) Carlos "Chacho" Álvarez (1996); 3) José A. Romero Feris (1996); 4) Antonio Tomás Berhongaray (1997); 5) Secretaría de Comunicaciones (2001); 6) Marta Osorio -1225-D-05- (2005); 7) Silvia Virginia Martínez 1798-D-05- (2005); 8) Andrés L. Sotos —985-D-05— (2005); 9) Delia Beatriz Bisutti —2032-D-06— (2006); 10) Dante Omar Canevarolo —3001-D-06— (2006); 11) Diana Conti y Agustín Rossi —2291-D-06— (2006). Tras ellas se inscriben el Proyecto de Ley de Reforma y Actualización Integral del Código Penal de la Nación (Resoluciones M.J. y D.H. nº 303/04 y nº 136/05), y el Proyecto de Ley (CD-109/06; S- 1751-1875 y 4417/06) y (Expediente 5.864-D.-2006) (2006).

3 La ley 26388 agregó tres párrafos a dicho precepto, que rezan del siguiente modo: "(e)l término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente". La ley 26733 añadió un último párrafo: "(e)l término 'información privilegiada' comprende toda información no disponible para el público cuya divulgación podría tener significativa influencia en el mercado de valores.

4 Riquert, Marcelo A.:"Delincuencia Informática en Argentina y el MERCOSUR", Ediar, Bs. As., 2009, p. 217.

5 Convenio sobre la ciberdelincuencia, Budapest, 23/11/2001, Serie de Tratados Europeos nº 185, Council of Europe / Conseil de l´Europe. Apenas en el corriente año, el Congreso de la Nación ha otorgado trámite legislativo a la solicitud de autorización para la incorporación de nuestro país a dicho instrumento internacional.

6 Vaninetti Hugo A.: "Inclusión del "Grooming" en el Código Penal", La Ley, Bs.As., 16/12/2013, AR/DOC/4628/2013. Del mismo autor, v."Media sanción del Senado al Proyecto de "Grooming", La Ley, Suplemento de Actualidad, Bs. As., 26/04/2012. 1; v. asimismo LO GIUDICE, María Eugenia: "Con motivo de la sanción de la ley que introduce el "delito de grooming" en el Código Penal (año 2013)", Suplemento de Derecho de Alta Tecnología de elDial.com. 2013, elDial.com - 11-12-2013 – DC1C0B.

7 Sueiro, Carlos Christian: "Criminalidad Informática. La eficiencia político-criminal de la reforma al Código Penal en materia de delitos informáticos. Análisis de las leyes 26.388, 26.685 y 26.904", Prólogo de Marcelo A. Riquert, AD-HOC, Bs. As., 2016, pp. 157/184.

8 La figura de apoderamiento ilegal a través de medios informáticos o tecnologías digitales había sido propuesta en tres de los proyectos de ley mencionados al comienzo de esta labor: en los de los diputados Carlos R Álvarez y José A. Romero Feris, ambos de 1996, y en el de este último legislador del año 2000.

9 La figura cobró significativa trascendencia a raíz del caso "Wikileaks". V. Domscheit-Berg Daniel: "Dentro de WikiLeaks. Mi etapa en la Web más peligrosa del mundo", Rocaeditorial, Bs. As., 2011. En nuestro país, con referencia al caso denominado "ArgenLeaks", v. O´Donnell, Santiago: "ArgenLeaks. Los cables de Wikileaks sobre la Argentina, de la A a la Z"., Sudamericana, Bs. As., 2011.

10 Tipo legal propiciado por la diputada Leonor Esther Tolomeo en su proyecto de 1996.

11 La opción de considerar comprendidos tales supuestos en base a las modificaciones terminológicas previstas en el citado artículo 77 del Código Penal de la Nación luce como una interpretación extensiva. V. sobre el tópico, PALAZZI P. A.: "Los

Delitos Informáticos en el Código Penal. Análisis de la ley 26.388", Abeledo Perrot, Bs. As., 2009, pp. 35/36.

12 Marcelo RIQUERT considera, en el mismo sentido: "sería importante que, para evitar los perniciosos efectos de la descodificación, como la falta de coherencia, de armonía y pérdida de proporcionalidad… se asumiera la profundización de la técnica de la última reforma… al que faltaría incorporar los tipos penales que en leyes especiales han quedado aislados, mejorando así su sistematicidad y orden".; en RIQUERT, Marcelo A.: "Delincuencia Informática en Argentina y el MERCOSUR", Ediar, Bs. As., 2009, p. 218.

13 RIQUERT M. A.: op. cit., pp. 202/204.

14 RIQUERT, M. A.: pp. 204/206.

15 PALAZZI Pablo A.: op. cit., pp. 159/166, se inclina por su no punición y su amparo a través del Derecho Civil. También RIQUERT, M. A., op. cit., 206/207, considera prudente y acertado postergar su punición hasta que exista un serio debate en torno a esta figura penal.

16 TOMEO, Fernando: "Responsabilidad penal de los administradores de sitios Web. El caso Taringa!", La Ley, Bs. As., 1º de Junio de 2011. V. también GRANERO, Horacio R.: "La naturaleza jurídica de la nube ("cloud computing")", en el Suplemento de Alta Tecnología de elDial.com, del 9/9/2009, elDial.com DC11A9; VELAZCO SAN MARTÍN, Cristo: "Aspectos jurisdiccionales de la computación de la nube", en el Suplemento de Alta Tecnología de elDial.com, del 14/4/2010, elDial.com DC1304; ELIZALDE MARÍN, Francisco: "La prueba en la Cloud Computing: Cloud Computing & Service Level Agreements. El modelo en los Estados Unidos de América y su proyección al ámbito local argentino", en el Suplemento de Alta Tecnología de elDial.com, del 8/6/2011, elDial.com DC15EE; TEIJEIRO Nicolás: "La protección constitucional de la intimidad en internet con especial referencia a redes sociales", en el Suplemento de Alta Tecnología de elDial.com, el 8 de junio de 2011, DC15EF.

17 V. AA.VV. – RIQUERT, Marcelo A. (coord.): *"Ciberdelitos"*, Hammurabi, Buenos Aires, 2015.

18 Además de la obra colectiva citada en la nota anterior, v. ABOSO, Gustavo Eduardo: *"Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación"*, BdeF, Bs. As. - Montevideo, 2017. También sobre la posible regulación de esta figura en la República Argentina, v. el artículo de PALAZZI, Pablo, en AA.VV. - DUPUY, Daniela (dir.), KIEFER, Mariana (coord..): *"CIBERCRIMEN. Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet"*., BdeF, Bs. As. - Montevideo, 2017.

19 V. AA.VV. - RIQUERT M. A. (coord..): op. cit.

20 MACHADO PELLONI, Fernando: *"Ciberodio",* en la citada obra de AA.VV. - RIQUERT MARCELO A. (coord..)

21 CHERÑAVSKY Nora A.:*"Responsabilidad penal de los proveedores de servicios de internet"., Revista Informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de Asociación Internacional de Derecho Penal (AIDP)*, Grupo Nacional, Facultad de Derecho, UBA, Bs. As.. 2014, pp. 17/32.

22 PETRONE, Daniel: op. cit.*"Prueba Informática"*, Didot, Bs. As., 2014.

23 SALT, Marcos: *"La relación entre persecución de los delitos informáticos y el Derecho Penal Internacional. Delitos Informáticos aspectos de Derecho Penal Internacional"*., en *Revista Informática y Delito, cit., pp. 237/245.*

24 SUEIRO Carlos Christian: *"La prueba digital en la criminalidad informática. A propósito del nuevo Código Procesal Penal"., en "El debido proceso penal".* LEDESMA, Ángela E. (dir.) – LOPARDO, Mauro (coord.), Hammurabi, Bs. As., nº 1, 2015, pp. 113/138.

25 Ricardo SÁENZ y Maximiliano RUIZ señalan tal deficiencia en estos términos: "(l) a reforma legislativa reviste una importancia central frente a la necesidad de readecuar las normas procesales,… ante el avance del ciberdelito y la falta de previsión legislativa ante las extendidas formas delictivas….La necesidad de reformular las reglas procesales sobre prueba digital se torna imperiosa, ya que si bien el uso de la analogía probatoria está permitido en materia procesal, resulta evidente la inconveniencia de seguir utilizando normas destinadas a otras situaciones (por ejemplo, intervenciones telefónicas) a realidades nuevas y con distintas connotaciones (por ejemplo, intervenciones de cuentas de correo electrónico). V. en: "Hacia un nuevo modelo de investigación en materia de ciberdelincuencia"., en el Suplemento de Derecho de Alta Tecnología de elDial.com. edición del 5/12/2012.

26 V. SUEIRO, Carlos Christian: "La Pena en la era digital. - A propósito de la introducción de la vigilancia electrónica en el nuevo Código Procesal Penal de la Nación (Ley 27.063)", Revista de Derecho Penal y Criminología, La Ley, Año VI, nº 4, Mayo 2016, pp. 159/170; del mismo autor: "La pena en la era digital – A propósito del futuro de la pena privativa de la libertad en la sociedad de la información"., en Revista de Ejecución de la pena privativa de la libertad y el encierro, Fabián Di Plácido, Bs. As., Año 10, nº 8, 2016, pp. 207/232, y "La Vigilancia Electrónica como forma de morigeración de la prisión preventiva. Alternativas a la prisión en la era digital",en Revista de Derecho Procesal Penal, "Alternativas a la prisión. Arresto Domiciliario. Interés Superior del Niño", año 2016 – 2, Rubinzal Culzoni, Santa Fé, 2017, pp. 105/156.

Brasil

Prof. Dr. Alexis Couto de Brito
Universidade Mackenzie- São Paulo

O debate no Brasil acerca dos delitos informáticos — ou delitos que envolvam tecnologias de informática — percorre três temas: 1) considerações sobre a parte geral do direito penal; 2) crimes comuns que são praticados por meio das novas tecnologias; e 3) delitos próprios que tem por bem jurídico as novas tecnologias.

I. Parte geral e delitos informáticos

A parte geral do direito penal brasileiro data de 1984, portanto, muito anterior à revolução tecnológica e principalmente à popularização da internet, que no Brasil ocorreu em meados dos anos 90.

Alguns problemas práticos são apontados quanto ao tempo e lugar do crime. Os delitos informáticos (praticados ou não pela internet) podem ter resultados muito

distantes do local de onde foi praticada a ação, podem ter seu resultado programado para execução automática e em determinada data, indeterminação com ralação à vítima ou ao número de vítimas atingidas, problemas de imputação de autoria e individualização das condutas praticadas. Todas estas questões também têm repercussões processuais com a indefinição da competência judicial para julgamento e colheita de provas. Os tribunais tem se manifestado em alguns casos, mas aleatoriamente e sem amparo na lei, como por exemplo, em delitos praticados pela internet a competência para o processo será o lugar do *upload* (STJ, 66981 / RJ), mas em furtos praticados contra depósitos bancários será o local físico no qual esteja situada a agência bancária (STJ, CC 86913 / PR).

Para determinação da pena algumas poucas previsões do Código penal podem ser interpretadas analogicamente e o juiz, utilizando-se do artigo 59[1] do Código (denominado circunstâncias judiciais) poderá aumentar a pena desde que fundamentadamente. Há previsão de aumento pelas "circunstâncias e consequências do crime" e pelo "comportamento da vítima", situações já utilizadas em alguns julgados para aumentar a pena em casos de subtrações múltiplas em fraudes bancárias.

II. Crimes comuns e as novas tecnologias

1. Delitos comuns que não sofreram alteração legal

Alguns delitos clássicos permitem a sua prática por meio das novas tecnologias. Os mais comuns são o furto, o estelionato, delitos contra a honra, apologia e incitação ao crime e crimes de preconceito.

Nos casos de furto há uma discussão doutrinária ainda não resolvida sobre a possibilidade do furto de dados ser adequado ao tipo penal do artigo 155[2]. Para alguns não se poderia incluir no conceito de "coisa" previsto no tipo algo imaterial e de duvidoso valor econômico como são os dados informáticos. A reforçar esta tese indicam a existência de uma lei de propriedade imaterial que trata dos delitos relacionados a marcas, patentes e invenções (Lei 9.279/96), bem como uma lei específica sobre software e programas de computador (Lei 9.609/98), o que aponta para uma necessidade de definição específica nesta matéria e que impediria a interpretação do elemento "coisa" como dados informáticos. Contudo, como tais leis não possuem a previsão do furto de dados, em oposição a este entendimento, seria possível a aplicação do furto previsto no artigo 155 em caso de subtração de dados quando houvesse valor econômico na informação subtraída (por exemplo, um catálogo de clientes) e a consequente eliminação do banco de dados original objeto da subtração, o que caracterizaria de fato a depreciação do patrimônio.

Não sendo o banco de dados o objeto direto da subtração admite-se a adequação ao tipo de furto e não ao de estelionato a subtração de valores de contas bancárias por meio de fraude e acesso não autorizado pela internet (STJ CAt.222/MG). Neste caso, aplicam-se inclusive as formas qualificadas do delito, a depender da conduta, como a previsão de rompimento de obstáculo, fraude ou emprego de chave falsa[3], pela transposição de firewall ou sistema de segurança equivalente, fazendo-se passar pelo verdadeiro usuário, utilizando login e senha originais substraídas da vítima, destreza, por especial habilidade para penetrar sem ser percebido, ou utilizando-se de chave falsa, por exemplo, a utilização de *keygen* ou *Cracks* para simular chaves originais de acesso. Nestes casos, cobra maior relevância a prova pericial para demonstrar a penetração do firewall (rompimento) ou a dissimulação da penetração (destreza), a utilização de máquina alheia ao usuário verdadeiro (endereço IP) e a invasão do sistema no qual a senha original era digitada, comparação da chave verdadeira e da falsa, apontando o software ou hardware utilizado ou capaz de ter sido utilizado.

Os delitos contra a honra, no Brasil, são delitos privados, o que significa que o Ministério Público não atua como promotor da ação penal, mas sim um advogado contratado pela vítima. É evidente que um delito contra a honra praticado pelas redes sociais tem um alcance diferenciado, e no Código penal brasileiro há uma previsão de aumento de pena se o delito é praticado por meio que facilite a divulgação[4]. Contudo, é causa extintiva da punibilidade para tais delitos a retratação da calúnia ou difamação proferida, pois sendo este ato praticado em público e perante o juiz a honra ofendida restaria integra novamente. Contudo, pelo alcance dado pelas redes sociais os tribunais não tem a admitido a simples retratação em audiência por não atingir a finalidade de publicidade equivalente à ofensa irrogada, exigindo que se dê publicidade também de maior proporção à retratação praticada[5].

2.2. Delitos comuns que sofreram alteração legal

Alguns delitos comuns já previstos na legislação brasileira sofreram alteração legal para prever a hipótese de serem praticados pela internet. É o caso dos crimes de preconceito de raça e cor (Lei 7.716/89), em especial o tipo do artigo 20 — incitação ao preconceito— que recebeu um parágrafo com pena de dois a cinco anos em casos nos quais o delito seja praticado por intermé-

dio dos meios de comunicação social ou publicação de qualquer natureza[6].

Outro delito objeto de adaptação foi o previsto no artigo 266 do Código penal —interrupção de serviço telegráfico, radiotelegráfico ou telefônico— que recebeu um parágrafo equiparando a serviço essencial o telemático ou de informação de utilidade pública[7].

As mudanças ocorreram no Estatuto da Criança e do Adolescente (Lei 8.069/90), na inviolabilidade dos segredos (arts. 153, §1º-A e 154-A do CPB), na inserção (art. 313-A) e modificação (313-B) não autorizada de dados, violação de sigilo funcional (art. 325).

Aos tipos penais já previstos na Lei 8.069/90 de produzir ou registrar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (art. 240) e ao de vender tais produções (art. 241) foram acrescentados outros quatro diretamente relacionados com a disponibilização do material pornográfico, seu armazenamento, distribuição e o aliciamento de crianças e adolescentes para fins libidinosos[8]. Nestes novos tipos, dois temas chamam a atenção. O primeiro diz respeito à imputação ao tipo do provedor de conteúdo que após ser comunicado oficialmente deixa de desabilitar o acesso ao conteúdo ilícito. O segundo, pela possibilidade de se punir por um delito aquele que simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia.

Ao artigo 153 foi apenas acrescentado o §1º para tipificar a divulgação de segredo mantido em bancos de dados pertencente ao governo[9]. O artigo 154-A foi introduzido no Código penal brasileiro após um fato de subtração de um aparelho celular do qual foi vítima uma atriz de televisão famosa. Em poucos meses foi aprovada uma lei que alterou o código penal e estabeleceu o tipo penal de invasão de dispositivo informático[10]. Estão compreendidas as condutas de invadir dispositivo rompendo sistema de segurança e implantar software malicioso para obtenção de vantagem ilícita. Também há previsão no parágrafo para quem produz, distribui, vende ou difunde software com tal capacidade.

Os artigos 313-A e 313-B foram incluídos após a descoberta de que o painel eletrônico que registrava as votações praticadas pelos parlamentares federais estava sendo manipulado para exibir resultado diferente do verdadeiro. Tipifica a inserção de dados falsos ou alteração de dados corretos de sistema de informática com o fim de obtenção de lucro ou sem autorização da autoridade competente[11].

Por fim, inclui-se no artigo 325 que prevê a violação de sigilo funcional o parágrafo 1º, para punir a conduta de permitir ou facilitar acesso a abanco de dados por empréstimo de senha e sua utilização sem autorização[12].

III. Bens jurídicos informáticos

A revolução tecnológica traz com ela condutas e resultados totalmente novos, e surge a preocupação com novos bens jurídicos virtuais, ou novas facetas de ataque a alguns bens jurídicos tradicionais como patrimônio, honra, fé pública etc. Podemos pensar em situações de apropriação de domínio alheio, desvio de DNS, Phishing, Spoofing, Pichação de Web sites, alteração de bancos de dados (páginas pessoais, Facebook, etc.), falsidade de documento eletrônico, furto de tempo de acesso, sobrecarga de fluxo de rede, fraude ou estelionato eletrônico, acesso não autorizado a banco de dados e até mesmo Cyber terrorismo.

Alguns destes comportamentos podem ser adequados aos parágrafos do artigo 154-A, como é o caso do acesso não autorizado a banco de dados (154-A, *caput*); danos a banco de dados (154-A, *caput* e §2º); furto de dados (154-A, *caput* e §3º); alteração de bancos de dados (154-A) em páginas pessoais como Facebook, pichação de Web sites e desvio de DNS; instalação de *Trojans* (154-a, *caput*); sobrecarga de fluxo de rede (266, §1º); fabricação e distribuição de códigos maliciosos (154-A, §1º); e Terminal Zumbi (art. 154-A, §3º)[13].

Outros porém como apropriação de domínio alheio, *Phishing, f*alsidade de documento eletrônico, furto de tempo, Spoofing e Cyber terrorismo ainda permanecem sem previsão legal ou possibilidade de interpretação analógica, configurando uma verdadeira lacuna no sistema jurídico penal brasileiro.

Notas

1 Art. 59: O juiz, atendendo à culpabilidade, aos antecedentes, à conduta social, à personalidade do agente, aos motivos, às circunstâncias e conseqüências do crime, bem como ao comportamento da vítima, estabelecerá, conforme seja necessário e suficiente para reprovação e prevenção do crime.

2 Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel.

3 Art. 155, § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:

I - com destruição ou rompimento de obstáculo à subtração da coisa;

II - com abuso de confiança, ou mediante fraude, escalada ou destreza;

III - com emprego de chave falsa;

IV - mediante concurso de duas ou mais pessoas.

4 Art. 141, III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.

5 CRIME CONTRA A HONRA. PENAL. RECURSO ESPECIAL. CALÚNIA. OFENSA VEICULADA NA INTERNET. EXI-

GÊNCIA DE PUBLICIDADE DA RETRATAÇÃO, QUE DEVE SER CABAL. RECURSO ESPECIAL IMPROVIDO.

1. Nos termos do art. 143 do Código Penal, a retratação, para gerar a extinção da punibilidade do agente, deve ser cabal, ou seja, completa, inequívoca.

2. No caso, em que a ofensa foi praticada mediante texto veiculado na internet, o que potencializa o dano à honra do ofendido, a exigência de publicidade da retratação revela-se necessária para que esta cumpra a sua finalidade e alcance o efeito previsto na lei.

3. Recurso especial improvido. (REsp 320.958/RN, Rel. Ministro ARNALDO ESTEVES LIMA, QUINTA TURMA, julgado em 06/09/2007, DJ 22/10/2007 p. 343).

6 Art. 20, § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: Reclusão de dois a cinco anos e multa.

7 § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

8 Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual.

Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso.

9 153, Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública

10 Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

11 Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente.

12 325, §1º, I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II – se utiliza, indevidamente, do acesso restrito.

13 Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Cybercrime In China

Yu, Jia Jia

Lecturer at KoGuan Law School, Shanghai Jiao Tong University, Ph.D in Law(the University of Tokyo), specializing in Criminal Law and Medical Law

In China, cybercrime encompasses a broad range of activities, including all crimes committed on the network by using a computer or similar electronic device (hereafter called a computer)[1]. Lawmaking in this field has a short history in China. The first part of this paper will introduce the three categories of cybercrime. The second part is the analyses of the increasing criminalization of actions endangering cybersecurity.

I. The Basic Construction

When the first criminal code of the People's Republic of China was enacted in 1979, there was no defini-

tion of cybercrime. At that time, the personal computer was not a common item in China.

Since the microcomputer revolution of the 1980s, which started in the USA, the personal computer was quickly introduced into China. The first criminal case, in which a computer was used as a tool for fraudulently withdrawing money from the victim's bank account, was reported in 1986. Since 1996 computer virus cases also began to emerge. Against this background, the criminal code was amended in 1997, and three articles prescribing cybercrime were newly added into Chapter VI, in which crimes of disrupting public order are clustered. There are three categories of cybercrime as below:

1. Article 285

The first category is called "offenses of illegally intruding". According to Article 285, whoever illegally intrudes into computer systems with information concerning state affairs, construction of defense facilities, and sophisticated science and technology (hereafter called three significant computer systems) shall be imprisoned for not more than three years. The act of illegally intruding, in itself, is serious enough to deserve criminal punishment.

For example, this article was applied in illegally intruding into "the information system of the Credit Reference Center of the People's Bank of China[2]"[3], into "the information system for Nationwide Professional and Technical Staffing Qualifying Exam Registration, which is managed by Ministry of Human Resources and Social Security of China"[4], into "the Traffic Information Management System, which is managed by Traffic Management Research Institute of the Ministry of Public Security"[5], and, into "the computer information systems of local governments"[6]. The first three systems are at a national level.

2. Article 286

The second category is called "offenses of illegally making damages". Three ways of making damages are respectively defined in Article 286.

(1) Article 286, Paragraph 1

When the target object is the computer information system, the act of making damages by illegally deleting, altering, adding, or interfering with the system can be a crime enumerated in paragraph 1.

For example, the offender accessed the computer Web server of the victim company and made changes to Nginx configuration[7]; or deleted and altered the backstage database of the "online to office" e-commerce platform[8]; or made DDoS attacks against gaming servers[9]; or attacked servers by using large flow[10]. There is another cluster of criminal cases, in which the offender accessed the system of the victim's iPhone and remotely locked it by changing the username and password for the purpose of blackmailing the victim for money to unlock the phone[11].

(2) Article 286, Paragraph 2

When the target object is the data or application programs installed in or processed and transmitted by the computer system, the act of making damages by illegally deleting, altering, or adding those data or application programs can be a crime enumerated in paragraph 2.

For example, the offender wrote a computer program and by using this program accessed the computer information system of a driving school to increase fraudulent data of the hours of studies[12]. In another case, when knowing the flaw in the network payment platform, the offender intercepted and altered data transmitted from his own computer to the cyberspace. By this method, when he paid 1 CNY into his account on this platform, he falsified the amount of the money by typing in 50,000 CNY[13].

(3) Article 286, Paragraph 3

According to paragraph 3, the act of making damages by deliberately creating and propagating computer viruses or other programs, which sabotage the normal operation of the computer system, can also be a crime.

First, "creating" does not mean that the offender must create the virus or program by himself/herself. In one criminal case, the offender ordered software, which is used for damaging or interfering in voice functionality, from another person, and sold this software online. He was convicted of this crime[14].

Second, "propagating" can also encompass differing activities, like "selling online" [15] "selling online and remote installing" [16] "deftly evading inspection systems and uploading the virus or program onto the Internet"[17] or, "sending a Trojan horse to a large number of the general public via SMS messaging"[18].

The act of making damages, in itself, is not serious enough to deserve punishment. In other words, in order to apply any paragraph in Article 286, the act of making damages must either cause grave consequences, or make the computer information system fail to run properly. Therefore, the punishment can be up to five years.

3. Article 287

The third category is called "offenses committed by using the computer as a tool". According to Article 287, whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes, shall be convicted and imprisoned according to relevant regulations of this crime. In fact, the crimes committed by using a computer many more than those mentioned above.

Relating to crimes of endangering national security enumerated in Chapter I in Special Provisions of Criminal Code, offenses of inciting ethnic hatred and discord, or offenses of organizing or directing the activities of splitting the nation, or offenses of stealing or leaking state secrets and military intelligence can be committed via the Internet.

Relating to crimes of undermining the order of socialist market economy in Chapter III, offenses of selling or making false propaganda for fake and shoddy goods; or offenses of fabricating and spreading fake inside information so as to have a major effect on the issuance and trading of the securities; or offenses of infringing the intellectual property, can also be committed via the Internet. And in some tax evasion cases, the offender deleted original data concerning business information written in emails of corresponding business partners, and cheated the tax administration by reporting a lower price. A wide range of online "peer-to-peer" (abbreviated P2P) financial platforms have emerged quickly in recent years. The network is a virtual world, and asymmetric information online creates high risks for investors. In more and more cases, offenders make use of P2P platforms to accumulate money from a crowd of investors in the name of "crowdlending" or "crowdfunding", but in fact they have no ability to pay back the money.

Relating to crimes of infringing upon citizen's rights to life, health and privacy in Chapter IV, more and more offenders using the Internet or cyber systems, to openly insult others or fabricate stories to slander others'or, to intercept, distort or delete the victim's e-mails or relevant data, so as to infringe upon his/her right of communication freedom or privacy. Online abuse usually causes real harm on a large-scale. Responding to this situation, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security (hereafter abbreviated SPC, SPP, MPS) issued *the Interpretation on Several Issues concerning the Specific Application of Law in the Handling of Defamation through Information Networks and Other Criminal Cases* (effective September 10, 2013).

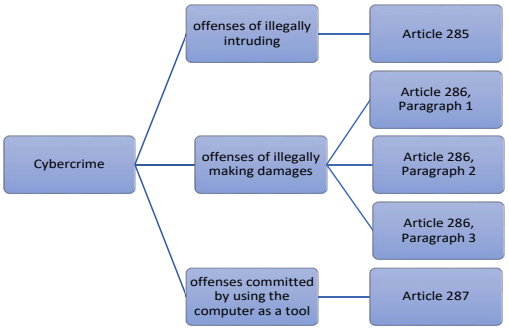
Crimes of encroaching on property, like online larceny, fraud and blackmail, are described in Chapter V, and, are the first cluster of crimes committed by using a computer or network. To settle those cases, SPC, SPP and MPS jointly issued two important official documents: *Announcement on Preventing and Cracking down on Crimes of Telecommunication Network-related Fraud* (effective September 23, 2016) and, *Opinions on Several Issues concerning the Application of Law in Handling Criminal Cases of Telecommunication Network-related Fraud* (effective December 19, 2016). The hard issue is about the protection of online virtual assets, which are intangible objects in online gaming and communities. Heated discussions are as to the interpretation of what is their legal status and how to protect them under criminal law. In the newest revision of General Provision of Civil Law (effective October 1st, 2017), it is declared that digital or online virtual assets are protected by law (Article 127). This marks the evolutionary development of the discussions mentioned above. But in criminal cases, the judge in SPC seemed reluctant to treat stealing virtual assets as equal to stealing traditional property[19].

Related to crimes of disrupting the order of social administration, Chapter VI describes three offenses that run rampant online. First, the Internet has made way for new types of gambling forms online. Responding to those new types of gambling, SPC, SPP and MPS jointly issued an official document, called *Opinions on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling* (effective August 31, 2010). In this document, it is held that whoever transmits gambling video, or data, and organizes gambling activities via the Internet, mobile communication terminals, etc., and falls under any of the following circumstances, shall be indicted of the crime of running a gambling house, as mentioned in Article 303 of Criminal Code: (i) establishing a gambling website and accepting bets; or (ii) establishing a gambling website and providing it for others to organize gambling; or (iii) acting as an agent of a gambling website and accepting bets; or (iv) participating in the profit sharing of a gambling website. Like making an occupation of gambling offline for the purpose of reaping profits, those acts committed online can also be indicted.

Second, the Internet has been used by drug traffickers and dealers for selling or buying drugs or raw materials (elixirs) for making drugs, for transmitting ways

of making compounds for drugs, or teaching manufacturing processes, and for scheming and directing other various drug-related offenses. "8.31 Case of Cyber-based drug trafficking and abusing on a large scale" is the first drug-related criminal case that described utilizing a web-based video chat platform for criminal activity. In this case, 12125 suspects were arrested, 144 criminal organizations were discovered, 340 drug dens were destroyed, 22 drug manufacturing factories were closed down, and 308.3 kilogram were seized.

Third, there are also more criminals creating porn websites, or assisting in the accessibility of those websites, or, disseminating obscene materials online, including e-books, e-journals, films and pictures, etc. SPC and SPP jointly issued *Interpretation (I) and (II) to solve Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations* (effective September 6, 2004 and February 4, 2010).



II. The Increasing Criminalization

Entering the 21st century, the number of Internet users in China has been rapidly increasing and reached 688,000,000 million in December of 2015[20]. Meanwhile, the Internet penetration rate in China went up to 50.3%, which means that more than half the people are using the Internet[21]. In this situation, the acts of committing or participating in the commission of cybercrime have been diversified. When amending criminal code in 2009 and in 2015, the legislator actively responded to this phenomenon by increasingly criminalizing of those acts.

1. Amendments to Article 285

In the 7th Amendment to Criminal Code (adopted February 28, 2009), two new articles were inserted in Article 285 as paragraph 2, and paragraph 3.

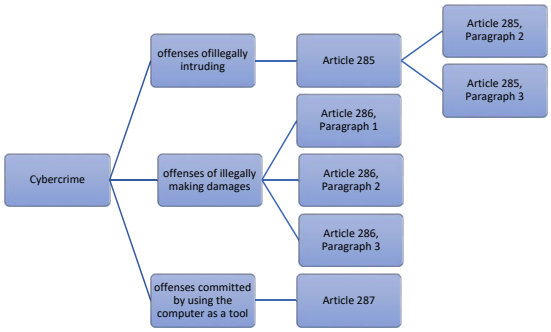
(1) Article 285, Paragraph 2

Based on paragraph 2, the act of intruding into a computer information system, other than three significant computer systems, is also criminalized. But the act of intruding, in itself, cannot constitute a crime. Two more requirements must be met. First, after intruding into the computer system, the offender must either, "obtain data in the computer information system", or, "control the computer information system". Second, the act must be deemed to have fallen under "serious circumstances"[22]. If the circumstances are extremely serious, the punishment can be up to seven years.

For example, in the following two cases, defendants were found guilty. In one case, after illegally logging into the Human Resources Website of Henan Province by the method of stealing the manager's username and password, the defendant obtained 370,000 items of personnel data information and sold the private information[23]. In the other case, the defendant made brute-force attacks against the victim's computer, and then infected their computer with a "Trojan horse", so as to succeed in controlling the computer information system[24].

(2) Article 285, Paragraph 3

According to paragraph 3, the act of knowingly providing special programs or tools used for intruding into or illegally controlling computer information systems, when the circumstances are serious, can be an individual crime. If there were no paragraph 3, the actor, who assists in committing the crime defined in paragraph 2, by providing programs or tools, could be convicted only when he/she conspires to commit the crime. But, according to paragraph 3, the supporter can be found guilty as long as he/she knows that the program or tool, which he/she provides, functions exclusively in the crime defined in paragraph 2[25], or that the person will use the program or tool, which he/she provides, to commit the crime defined in paragraph 2[26]. In the latter situation, the program or tool does not have to function exclusively in the crime defined in paragraph 2. In both situations conspiracy is not needed.



2. Amendments to Article 286

In the 9th Amendment to the Criminal Code (effective November 1, 2015), a new paragraph was added after Article 286 as Article 286 A. According to this article, any network service provider, who fails to perform the information network security management duties, and upon being ordered by the oversight and management department to adopt rectification measures still do not make correction, can be charged with a crime.

This is a crime committed by omission. Objectively speaking, the network service provider assists in another perpetrator's commission of cybercrime by omission. But subjectively speaking, the provider does not conspire with another perpetrator. Regarding the act of the network service provider, two possibilities exist. The first is that he/she has a unilateral intention of assisting in another's commission of cybercrime. The second is that he/she can generally foresee the risk created by his/her omission, but takes no measures to avoid it. Especially in the latter situation, no person will be prosecuted as an accessory only for his/her assisting in another's commission of crime with negligence. However, Article 286 A explicitly criminalizes unilaterally assisting in, and recklessly, or negligently, assisting in another's commission of cybercrime.

The duties should be those provided by laws or administrative regulations, of which the most important is *Cybersecurity Law of China* (effective on June 1, 2017). Article 21 of this law prescribes the following duties: (i) Developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection; (ii) Taking technical measures to prevent computer viruses, network attacks, network intrusions and other acts endangering cybersecurity; (iii) Taking technical measures to monitor and record the status of network operations and cybersecurity incidents, and preserving relevant weblogs for not less than six months as required; (iv) Taking measures such as data categorization, and back-up and encryption of important data; (v) Performing other obligations as prescribed by laws and administrative regulations. The official docume nts as below are also usually taken into account: *Provisions on the Administration of Internet Live-Streaming Services* issued by the State Internet Information Office (effective December 1, 2016); *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks* adopted at the 30th Session of the Standing Committee of the Eleventh National People's Congress (effective December 28, 2012); *Administrative Measures for the Security Protection of Computer Information Networks Linked to the Internet* approved by the State Council (revised on January 8, 2011).

The omission of the network service provider deserves punishment only when it results in one of the following serious consequences: (i) causing the spread of a large amounts of illegal information; or (ii) causing the leakage of users' information, with serious consequences; or (iii) causing the loss of criminal case evidence, with serious circumstances; or (iv) any other serious circumstance. The punishment can be up to three years.

3. Amendments to Article 287

In the 9th Amendment to Criminal Code, two new paragraphs were added after Article 287 as Article 287 A and Article 287 B.

(1) Article 287 A

According to Article 287 A, making use of network technology to teach the way of, or to facilitate the commission of crimes, by taking the following measures, can be an individual offense. Those measures include (i) setting up a website or mail list for the purpose of committing fraud, transmitting criminal methods, making or selling prohibited or controlled items, or engaging in other illegal activities; or (ii) spreading illegal information related to producing or selling drugs, guns, obscene items or other prohibited or controlled items; or (iii) spreading information for committing fraud or other illegal activities. The punishment can be up to 3 years.

In consideration of the elements of a crime, in most cases, those measures, as mentioned above, show the behavior of merely preparing for the commission of a crime, and therefore, may create only abstract risks to

the interest protected by law. Before the 9th Amendment to Criminal Code was effective, it was hard to say that taking those measures always deserved criminal punishment. But now, based on Article 287, taking those measures in itself has been criminalized. For example, in a cluster of criminal cases, offenders, who either were hired by fraudsters, or followed fraudsters' instructions, sent out text messages to a large number of the general public pretending to be from a *bank or* a telecommunication cooperation, and then were found guilty[27].

When applying Article 287 A, the judge has to make judgment as to whether taking those measures can be regarded as an attempted offense, which have proceeded beyond the stage of preparing for a crime. When taking those measures in an attempted offense, e.g. an attempted fraud, the accomplished crime according to Article 287 A, and the attempted crime of fraud according to Article 266, exist together'in German it is called "Idealkonkurrenz". In this case, the judge in China will adopt the heavier punishment on basis of Article 266. In several cases, fraudsters, who attempted to send out text messages pretending to be from a bank or a telecommunication cooperation, were convicted of attempted fraud[28].

(2) Article 287 B

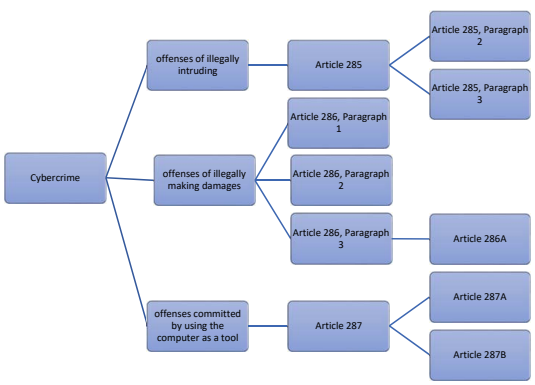
According to Article 287 B, knowingly providing technical support or material help to online criminals has also been criminalized. The punishment can be up to three years.

"Technical support" refers to Internet access, server hosting, web storage, or communications transfer, etc. "Material help" refers to providing help such as in advertising and promotions or paying bills. All those supporting activities belong to normal service offered for cyber consumers, which are in themselves harmless. Nevertheless, when the actor engages in those activities, and consequently assists in another's commission of cybercrime, he/she can be found guilty, as long as he/she knows his/her consumers are online criminals, even though he/she has no intention of assisting in another's commission of cybercrime, or has no intention of conspiring with online criminals.

For example, the offender knew his cyber acquaintance was in the process of committing telecommunication fraud through a phishing site, but still sold him domain names and helped to analyze data[29]; or, the offender knew that X was committing an offense of illegally controlling computer information system, but still remote logged into the management server, to assist in X's maintenance of the controlled computer system, and provided an account to X for payment and settlement[30]; or, the offender, who rented out local phone numbers online, knew that some customers were using phone numbers to commit fraud, but, profited through information transmission technology[31].

It is not necessary that the offender knew another's commission of crime from the beginning. In one case, the offender, who rented out phone circuits, received an official document from the telecommunication company, in which he was warned that certain circuits were suspected of being involved in fraud, and was ordered to take measures against it. The offender knew who was using this circuit, but did not take the necessary measure but for transferring the official document to the rental[32]. In those cases, as mentioned above, the crime, which the offender assisted in, first existed and was committed individually. The offender didn't participate in the planning, organizing or preparing for the crime, and therefore, his act of providing technical support, or material help, played a very small role.

In the opposite, if the offender participates more actively in or made greater contributions in the commission of cybercrime, his/her act can also constitute the crime of fraud. In this case, he/she should be convicted of fraud with a heavier punishment[33]. For example, the offender discovered the security flaw in the electronic network platform of his company, and conspired a plan to cheat customs of their money by using this flaw. In order to place this plan into motion, the offender registered a new company and bought an electronic business platform in the name of this company. Later, the offender transferred possession of the company, the platform and its management server to Y who had the same intention. Y used this platform to commit fraud. In this case, the offender was determined to be an accomplice in the crime of fraud committed by Y, and was convicted of fraud[34].



III. Conclusion

With the emergence of computer systems in China, cybercrimes have rapidly evolved in sophistication in the country. Within the last ten years, the field of lawmaking, and rulemaking activities, has been active in addressing these activities, and criminal cases have emerged quickly.

In the new amendments, the most attractive feature lies in the increasing criminalization of the acts of positively assisting in the commission of cybercrime (paragraph 3 of Article 285 and Article 287B), of negatively assisting in cybercrime by omitting to take measures to guarantee the safety of networks (Article 286 A), and, of preparing for the commission of cybercrime (Article 287 A). To sum up, punishments for cybercrimes in China are steadily becoming harsher and harsher.

Notas

1 Article 1 in *Opinions on Several Issues concerning the Application of Criminal Procedures in the Handling of Cybercrime Cases*, which was issued on May 4th, 2014 by the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security.

2 The People's Bank of China is the central bank of China, which formulates and implements monetary policy and supervises and regulates the financial industry.

3 nº 278 Criminal Judgment made on September 22, 2016 by the local people's court in Shangshui County of Henan Province.

4 nº 34 Criminal Judgment made on April 2, 2014 by the local people's court in Jinan High-tech Industrial Development Zone of Shandong Province.

5 nº 260 Criminal Judgment made on August 19, 2014 by the local people's court in Lizhou district, Guangyuan City of Xichuan Province.

6 nº. 246 Criminal Judgment made on March 27, 2015 by the local people's court in Changxing Country of Zhejiang Province.

7 nº. 239 Criminal Judgment made on July 12, 2016 by the local people's court in Tongzhou District of Beijing Municipality.

8 nº 686 Criminal Judgment made on October 20, 2016 by the local people's court in Gulou District, Nanjing City of Jiangsu Province.

9 nº 79 Criminal Judgment made on May 5, 2016 by the local people's court in Wuxi City of Jiangsu Province; nº 174 Criminal Judgment made on July 6, 2016 by the local people's court in Yuanzhu District, Yichun City of Jiangxi Province; nº 380 Criminal Judgment made on February 14, 2017 by the local people's court in Binjiang District, Hangzhou City of Zhejiang Province.

10 nº 157 Criminal Judgment made on May 31, 2016 by the local people's court in Binjiang District, Hangzhou City of Zhejiang Province.

11 nº 548 Criminal Judgment made on January 20, 2017 by the local people's court in Haian Country of Jiangsu Province; nº. 660 Criminal Judgment made on January 9, 2017 by the local people's court in Qidong City of Jiangsu Province; nº 495 Criminal Judgment made on July 26, 2016 by the local people's court in OuhaiDistrict, Wenzhou City of Zhejiang Province; nº. 391 Criminal Judgment made on November 16, 2016 by the local people's court in Yuhuan Country of Zhejiang Province.

12 nº 19 Criminal Order of final Instance made on April 19, 2016 by the intermediate people's court in Taizhou City of Jiangsu Province.

13 nº 75 Criminal Judgment made on March 17, 2017 by the local people's court in Deqing Country of Zhejiang Province.

14 nº 332 Criminal Judgment made on November 11, 2016 by the local people's court in Yuhuatai District, Nanjing City of Jiangsu Province.

15 Id.

16 nº 182 Criminal Order of Final Instance made on November 19, 2015 by the intermediate people's court in Yinchuan City of Ningxia Hui Autonomous Region.

17 nº 192 Criminal Judgment made on March 30, 2016 by the local people's court in Dongcheng District of Beijing Municipality.

18 nº 307 Criminal Order of Final Instance made on November 15, 2016 by the intermediate people's court in Chengde City of Hebei Province.

19 HU, Yuteng, ZHOU, Jiahai and ZHOU, Haiyang: *How to Understand and Apply "the Interpretation on Several Issues concerning the Application of the Law in the Handling of Theft Criminal Cases"*, 15 The People's Judicature(2014). The authors are the judges of the Supreme People's Court.

20 The 37th Report issued by CNNIC about the Internet Development Situation in China, in: http//tech.sina.com.cn/i/2016-01-22/doc-ifxnuvxh5133709.shtml [2016-02-20].

21 Id.

22 According to *the Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems* issued by SPC and SPP (effective on September 1st, 2011), in one of the following situations, the circumstances can be admitted serious: (i) Obtaining 10 or more groups of identity verification information used for payment and settlement, securities trading, futures trading and other online financial services; (ii) Obtaining 500 or more groups of identity verification information other than that mentioned in item; (iii)Illegally controlling the information systems of 20 or more computers; (iv) Obtaining illegal income of 5,000 CNY or more or causing economic losses of 10,000 CNY or more; or (v) Other serious circumstances.

23 nº 123 Criminal Order of Final Instance made on December 6, 2013 by the intermediate people's court in Huzhu City of Zhejiang Province.

24 nº 578 Criminal Judgment made on December 26, 2016 by the local people's court in Huishan District, Wuxi City of Jiangsu Province.

25 nº 44 Criminal Order of Final Instance made on March 10, 2017 by the intermediate people's court in Changzhu City of Jiangsu Province.

26 nº 00087 Criminal Judgment made on March 3, 2011 by the local people's court in Huoqiu Country of Anhui Province.

27 nº 1663 Criminal Judgment made on November 30, 2016 by the local people's court in Futian District, Shenzhen City of Guangdong Province; nº. 84 Criminal Judgment made on September 23, 2016 by the local people's court in Jishou City of Hunan Province; nº 208 Criminal Judgment made on September 13,

2016 by the local people's court in Xiling District, Xichang City of Hubei Province; nº 314 Criminal Judgment made on September 5, 2016 by the local people's court in Jindong District, Jinhua City of Zhejiang Province; nº 52 Criminal Judgment made on August 30, 2016 by the local people's court in Jishou City of Hunan Province.

28 nº. 111 Criminal Order of Final Instance made on September 13, 2016 by the intermediate people's court in Ezhou City of Hubei Province; nº 572 Criminal Order of Final Instance made on July 21, 2016 by the intermediate people's court in Jinhua City of Zhejiang Province; nº. 437 Criminal Judgment made on March 2, 2017 by the local people's court in Dongchangfu District, Liaochen City of Shandong Province; nº. 134 Criminal Judgment made on September 28, 2016 by the local people's court in Qihe Country of Shandong Province.

29 nº. 968 Criminal Judgment made on December 20, 2016 by the local people's court in Pujiang Country of Zhejiang Province.

30 nº 578 Criminal Judgment made on December 26, 2016 by the local people's court in Huishan District, Wuxi City of Jiangsu Province.

31 nº 1032 Criminal Judgment made on February 16, 2017 by the local people's court in Tuecheng District, Shanxing City of Zhejiang Province.

32 nº. 00026 Criminal Judgment made on November 23, 2015 by the local people's court in Binhu District, Wuxi City of Jiangsu Province.

33 nº 1084 Criminal Order of Final Instance made on April 1, 2017 by the intermediate people's court in Hangzhou City of Zhejiang Province.

34 nº 22 Criminal Order of Final Instance made on September 29, 2016 by the intermediate people's court of the nº. 6 Xinjiang Production and Construction Corps.

Colombia

Álvaro Orlando Pérez Pinzón

Exmagistrado y expresidente de la Sala de Casación Penal de la Corte Suprema de Justicia.

Miembro de la Academia Colombiana de Jurisprudencia

1. Lo fundamental de las conductas problemáticas conocidas como criminalidad informática se halla en la Ley 1273 del 2009, "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico —denominado De la protección de la información y de los datos— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Esta ley, que se incorporó al Código Penal, además, creó otro Título del Libro Segundo del mismo estatuto, al que bautizó como Título VII (bis), "De la protección de la información y de los datos", inmediatamente después del Título VII, que se ocupa en los delitos contra el patrimonio económico. El nombre básico del Título, "Protección de la información y de los datos", coincide plenamente con la denominación que se estableció y se explicó desde la Exposición de Motivos de los proyectos de ley que luego se convirtieron en la ley 1273 del año indicado[1].

2. Los artículos finalmente aprobados e incrustados en el Código Penal fueron los siguientes:

Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

ARTÍCULO 269A. *ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269B. *OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN*. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

ARTÍCULO 269C. *INTERCEPTACIÓN DE DATOS INFORMÁTICOS*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de 36 a 72 meses.

ARTÍCULO 269D. *DAÑO INFORMÁTICO*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269E. *USO DE SOFTWARE MALICIOSO*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269F. *VIOLACIÓN DE DATOS PERSONALES*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269G. *SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de 1/3 a la 1/2, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

ARTÍCULO 269H. *CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA*. Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Atentados informáticos y otras infracciones

ARTÍCULO 269I. *HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

ARTÍCULO 269J. *TRANSFERENCIA NO CONSENTIDA DE ACTIVOS*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de 48 a 120 meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

3. Aparte la legislación básica que se acaba de reseñar, el tema también ha sido atendido en el Código Penal para otros efectos, por ejemplo en las siguientes disposiciones:

3.1. Artículo 58.17, como circunstancia *genérica* de mayor punibilidad: la pena se agrava cuando para la realización de las conductas punibles se utilicen *medios informáticos, electrónicos o telemáticos*.

3.2. Artículo 193, residual, que sanciona el ofrecimiento, venta o compra de instrumentos aptos para interceptar la comunicación privada entre las personas.

3.3. Artículo 195, derogado por el artículo 4º de la Ley 1273 del 2009, que preveía multa para quien accediera abusivamente a un sistema informático. Su contenido fue absorbido por el artículo 269 A de la Ley 1273 del 2009.

3.4. Artículo 218.2, que intimida con prisión y multa a quien "alimente con pornografía infantil *bases de datos de internet*, con o sin fines de lucro" (con las modificaciones hechas por los artículos 12, de la ley 1236 del 2008, y 24 de la ley 1336 del 2009).

3.5. Artículo 223, que intensifica la pena para la injuria y la calumnia cuando se cometen utilizando *cual-*

quier medio de comunicación social u otro de divulgación colectiva.

3.6. Artículo 240, inciso 5º, que califica el hurto si se comete sobre elementos destinados a comunicaciones telefónicas, telegráficas, *informáticas*, *telemáticas* y *satelitales*.

4. Una comparación sencilla de la normativa anterior permite concluir que nuestro legislador estuvo cerca del Convenio de Budapest sobre cibercriminalidad, del 2001-2004, lo cual es obvio pues este instrumento, sin duda, quiere agotar al máximo la temática. Colombia, como otros países, entonces, parece seguir la misma línea. Sin embargo, surge una curiosidad: Colombia solicitó al Consejo de Europa la invitara a formar parte del Convenio. Fue convidada pero hasta la fecha[2] no ha adherido como sí lo han hecho otros Estados no europeos, que ya lo han adoptado o se enrumban por esa vía, entre ellos México, El Salvador, Costa Rica, Argentina, Uruguay, Chile, República Dominicana, Perú, Estados Unidos de América, Canadá y Japón[3].

5. Como se puede ver, para el mundo actual, concretamente para Colombia, el primer paso del proceso de criminalización, el de creación de la ley, parece suficiente en materia telecomunicativa e informática. Otra cosa es que la segunda etapa de ese proceso, la aplicativa, aún no enseñe suficiente material como para poder tratar de calificar la trascendencia real de la legislación adoptada. Lo mismo sucede, entonces, con la tercera fase de tal proceso, es decir, la de ejecución penitenciaria. Será necesario esperar otros días.

Notas

1 En la Cámara de Representantes, proyectos 042 y 123 del 2007, y en el Senado de la República, proyecto de ley 281 del 2008.

2 Mes de mayo del año 2017.

3 Como se suele decir, el tiempo apremia pues la invitación se hizo hacia el año 2013 y la posibilidad se agotaría en el 2018. Sin embargo, al menos, existe un proyecto de ley atinente al Convenio.

Costa Rica

Roberto Madrigal Zamora

I. Aspectos jurídicos

La actual legislación costarricense en materia de delitos informáticos o ciberdelincuencia puede sistematizarse según los siguientes datos: adición al Código Penal de los artículos 196 bis, 217 bis y 229 bis del Código Penal mediante Ley N°8148 de 24 de octubre de 2001 para reprimir y sancionar los delitos informáticos; reforma posterior mediante Ley 9048 del 10 de julio de 2012 introduciendo al mismo cuerpo de leyes la Sección VIII "Delitos Informáticos y Conexos" del Título VII del Código Penal*;* y reforma posterior mediante Ley N° 9135 del 24 de abril de 2013).

Así, las figuras típicas contenidas en el mencionado código sustantivo son las siguientes:

"**Artículo 229 bis.- Daño informático.**

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable".

"**Artículo 229 ter.- Sabotaje informático.**

Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático".

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

"**Sección VIII**

Delitos informáticos y conexos

Artículo 230.- Suplantación de identidad.

Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información".

"**Artículo 231.- Espionaje informático.**

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio".

"**Artículo 232.- Instalación o propagación de programas informáticos maliciosos.**

Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.

b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.

c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.

d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.

ii) Afecte el funcionamiento de servicios públicos.

iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.

iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático".

"**Artículo 233.- Suplantación de páginas electrónicas.**

Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero".

"**Artículo 234.- Facilitación del delito informático.**

Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos".

"**Artículo 235.- Narcotráfico y crimen organizado.**

La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado".

"**Artículo 236.- Difusión de información falsa.**

Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios".

El llamado Convenio de Budapest -documento internacional que disciplina el tema en cuestión- fue aprobado por la Asamblea Legislativa costarricense en primer debate en fecha 20 de febrero de 2017 y se encuentra actualmente pendiente de aprobación en segundo debate.

Una rápida revisión de la jurisprudencia nacional muestra que el tipo penal sobre el que en apariencia ha versado mayormente la discusión en la resolución de casos lo es el Fraude Informático a cuyo tenor se han sancionado conductas como la de:

– imponerse por medios informáticos de los datos de usuario y contraseña de usuarios de entidades bancarias y el ingreso por esa vía a los sistemas de internet para lograr el traslado de fondos de una cuenta a otra; actividad que se ha interpretado calza en el concepto "influir en el procesamiento de datos de un sistema de cómputo mediante el uso indebido de datos";

– el uso de tarjetas de débito bancarias que permiten el acceso a cajeros automáticos, situación sobre la cual se ha presentado una discusión en el sentido de si se esta en presencia de un delito de hurto equiparándose dicha tarjeta con una llave;
– la contribución al cometimiento del delito mediante la acción de brindar los datos de una cuenta bancaria que serviría de destino para un traslado fraudulento de fondos y realizar el retiro del dinero con lo cual se ha considerado que se compartió el dominio funcional del hecho y por lo tanto se constituye una situación de coautoría;
– la toma ilegal de los datos de las bandas magnéticas de tarjetas de crédito los cuales una vez codificados en otras tarjetas espúreas se utilizan en diversos comercios para la adquisición de bienes y servicios.

II. Aspectos criminológicos

En la llamada era de la información y la globalización es obvia la relevancia que los instrumentos tecnológicos asumen en todo el desenvolvimiento de la vida cotidiana, tanto a nivel microsocial como macrosocial y es obvio también que por lo mismo este es un tema en que las economías centrales tienen un marcado interés en dictar pautas a nivel mundial como lo hacen en el tema del narcotráfico. Este interés se traduce en la organización de actividades regionales de capacitación, la dotación de recursos oficiales a las agencias policiales, el impulso a la firma de tratados y documentos internacionales de persecución penal, el ejercicio de un poder global de policía a través de la calificación de la actividad de persecución del delito efectuada por los gobiernos periféricos con las consecuentes felicitaciones o censuras que pueden traducirse incluso en sanciones o consecuencias económicas, etc.

No hay que ir muy lejos para determinar como pese al poderío económico, militar y político de estas economías centrales se muestran vulnerables frente al uso que de manera contestataria (ya sea legítima o no) se le puede dar a las herramientas tecnológicas, recuérdese nada más el llamado Caso Wikileaks o las recientes revelaciones de filtraciones de información o hackeo nada más y nada menos que en torno a la campaña presidencial de los Estados Unidos de Norteamérica.

Como si esto ya no fuera suficiente para que exista una marcada tendencia a la penalización, el tema de las posibilidades de trasiego y producción de información por la vía del uso de las tecnologías toca intereses relacionados con sectores de presión que desde hace tiempo vienen propugnando por el uso del derecho penal como el caso de los activistas por los derechos de las mujeres y los menores de edad, los representantes de los intereses económicos relacionados con la propiedad intelectual o los activistas por los derechos de poblaciones sexualmente diversas.

En este sentido piénsese en todo lo relacionado con la pornografía infantil, la reproducción y difusión masiva de obras artísticas, la difusión de posiciones discriminadoras y fomentadoras del odio por cuestiones étnicas o de preferencia sexual, etc.

Otro tema del orden de lo criminológico que se ha puesto sobre el tapete en el foro nacional es el de la posible asignación de responsabilidad penal a las plataformas sociales o a las redes sociales en lo que vendría a ser toda una revolución de los paradigmas propios del derecho penal republicano.

Desde otra arista de la vertiente criminológica y más a tono con la perspectiva que como defensor público ejerzo, este es un tema más en que como todos los que tienen que ver con delincuencia organizada probablemente los que se vean sometidos al poder punitivo del estado sean aquellos eslabones de la cadena con menor poder y provecho de la actividad delictiva, siendo de temer además que servicios de defensa como precisamente el de la defensa pública se tenga que enfrentar a la persecución penal con recursos exiguos que no le permiten el acceso efectivo a consultores técnicos y peritos en un tema esencialmente especializado.

España

Elena Núñez Castaño
Profesora Titular de Derecho Penal de la Universidad de Sevilla

I. Consideraciones generales: concepto de *ciberdelito*

La característica principal del siglo XXI es el impacto de las nuevas tecnologías en la sociedad, y el progreso informático. De este modo nos encontramos ante lo que se ha dado en denominar *sociedad de la información y la tecnología*, precisamente a causa del enorme impacto que los avances tecnológicos han tenido en el desarrollo de la vida cotidiana de la sociedad actual. Y ello ha determinado que nuestra sociedad y nuestra realidad cambien de manera radical. Como señala GALÁN MUÑOZ[1] *"Vivimos tiempos de cambios; tiempos en los que las viejas realidades nacionales son cada vez más puestas en entredicho por fenómenos políticos,*

económicos y técnicos a los que no pueden hacer frente por sí solas". Y uno de estos fundamentales cambios lo ha representado la informática, las nuevas tecnologías de la información y de la comunicación, que han revolucionado nuestro entorno social, económico, político y, obviamente también, jurídico.

Así las nuevas tecnologías de la Información y de la Comunicación (TIC´s) aparecen como un poderoso instrumento de ordenación y obtención de información[2], pero sobre todo de comunicación e incluso de actividad financiera y económica se ha volcado de manera relevante en lo que se ha dado en denominar *ciberespacio*[3], de manera que el nivel de transacciones económicas y de negocios ha crecido exponencialmente a través de este medio de comunicación global[4]. Y ello no tiene perspectivas de retroceder, sino que irá aumentando conforme pase el tiempo *"con los sistemas informáticos como forma de trabajo y también de diversión, con las redes sociales como forma de interactuación social, con las tecnologías móviles totalmente conectadas y con toda la información en la palma de la mano, el ciberespacio como lugar de encuentro por el uso de las TIC's irá expandiéndose"*[5].

Ahora bien, esas mismas tecnologías que sirven para facilitarnos la vida y la comunicación en el quehacer cotidiano, pueden determinar afectaciones y vulneraciones importantes de los derechos de los ciudadanos en cuanto sean utilizadas de manera abusiva para vulnerar los mismos. Es decir, las mismas facilidades que implican para el desarrollo de la vida diaria, son las que suponen para la comisión de cualquier tipo de actividad delictiva o contraria al ordenamiento jurídico que suponga o pueda suponer una vulneración de los derechos de los demás ciudadanos. O dicho de otro modo resulta innegable que los cambios sociales que estamos viviendo derivados de los importantes cambios y avances tecnológicos han determinado la aparición de una serie de comportamientos que se realizan mediante la utilización de las TIC´s y que determinan tanto nuevas modalidades delictivas por atentar contra nuevos intereses dignos de tutela penal como pudiera ser la seguridad en el uso de sistemas informáticos, como nuevos medios de ataque contra bienes jurídicos tradicionales, como la estafa informática o los daños informáticos, etc.

De este modo, la delincuencia a través de estas tecnologías o ciberdelincuencia surge de manera inevitable como una nueva realidad social; y esta realidad social ha ido evolucionando del mismo modo en que han evolucionado estas nuevas tecnologías[6] hasta que hoy en día, y debido al enorme protagonismo que han adquirido las redes sociales y otras formas de comunicación personal que implican una clara e importancia cesión de amplias parcelas de intimidad personal, así como un incremento de la relaciones personales en el ciberespacio y el aumento de la actividad económica en internet, *"asistimos a un momento álgido de la criminalidad en el ciberespacio, tanto en sentido cuantitativo dado el creciente uso de Internet en todo el mundo y por todo el mundo, como cualitativo al aparecer nuevas formas de delincuencia relacionadas con los nuevos servicios y usos surgidos en el entorno digital"*[7].

Paralelamente a la evolución de los comportamientos delictivos mediante las nuevas tecnologías, se ha producido la de la evolución de sus autores. De esta manera, hemos pasado del delincuente individual caracterizado esencialmente como una persona joven, casi adolescente, introvertido, con problemas de relaciones sociales que, por el contrario, se convertía casi en un héroe en el ciberespacio (el mítico *hacker*), a organizaciones criminales dedicadas a la cibercriminalidad que emplean los avances y facilidades de las nuevas tecnologías para ampliar su ámbito de actuación y aumentar sus actividades ilícitas y sus recursos. De esta manera, se sustituye el espacio físico por el virtual, pero la criminalidad sigue siendo la misma. Al mismo tiempo, surge una nueva modalidad de ciberdelitos, los *sociales*, que basándose en la utilización de Internet y redes sociales, convierten en potencial sujeto pasivo a cualquier ciudadano que utilice estas nuevas tecnologías y que podría ver lesionadas su honor, libertad sexual, intimidad, etc.; similares situaciones podrían producirse mediante la utilización de las nuevas tecnologías para atentar contra la seguridad pública, como el caso del ciberterrorismo o los ataques masivos contra sistemas informáticos.

Esta ampliación de las posibilidades de ataque a diversos bienes jurídicos mediante el recurso a las nuevas tecnologías ha determinado que los ordenamientos jurídicos hayan incorporado específicas modalidades informáticas de ataque a bienes jurídicos tradicionales, así como figuras concretas de tutela de la seguridad informática[8]; incorporación que, en la mayor parte de las ocasiones ha determina un adelantamiento injustificado e ilegítimo de la intervención penal en aras de una mayor prevención que conlleva claramente la limitación de los derechos y libertades de los ciudadanos. De este modo, en España se han ido introduciendo conductas caracterizadas por el uso de medios informáticos desde la aprobación del Código penal de 1995 (como ocurrió con la estafa informática), que se han aumentado paulatinamente con las sucesivas reformas como las de 2010 y 2015. Reformas que consisten en la trasposi-

ción, casi literal de distintos instrumentos internacionales sobre la tutela de la seguridad informática[9], y que conllevan, como muy acertadamente señalaba GALÁN MUÑOZ[10] que el legislador acuda a ellas como justificación de la criminalización de conductas *"alejadas de la efectiva lesión del bien jurídico que supuestamente pretende proteger con su tipificación"* sin que importe que, con ello, se esté vulnerando *"las más básicas exigencias derivadas de principios penales tan esenciales como el de intervención mínima o el subsidiariedad, ni con las derivadas de otros más generales como el de proporcionalidad. Todo parece quedar olvidado desde el mismo momento en que se alude a su ascendiente u origen internacional"*.

Es por ello que los problemas de legitimidad que comportan muchas de estas "nuevas" modalidades típicas resultan innegables, y no quedan justificados ni mucho menos por la referencia a las obligaciones internacionales que acostumbra a realizar el legislador nacional; sin embargo, ello no ha supuesto problema alguno a la hora de incorporar a nuestro ordenamiento jurídico penal nuevas conductas *"referidas al uso o al abuso de las modernas tecnologías de la información"*[11].

Ante esta realidad, se hace necesario, en primer lugar, aportar un breve análisis de lo que deba entenderse por *ciberdelito* o *delito informático*, y en segundo lugar, una enumeración de cuales son las principales y más relevantes manifestaciones de este fenómeno de cibercriminalidad que se encuentran tipificadas como delitos en nuestro Código penal.

Una vez superada la denominación de *delitos informáticos*[12] que se utilizó por la doctrina desde mediados del siglo pasado hasta principios de éste, se ha sustituido por la expresión *ciberdelito* o *cibercrimen*[13] que hace referencia a toda aquella delincuencia que se encuentra relacionada con el empleo de las TIC´s. Así, a diferencia de los delitos informáticos, este fenómeno de la *cibercriminalidad* ya no tiene su elemento característico en que se realice desde o mediante un ordenador, sino *"por el hecho de que tales sistemas informáticos estén conectados en un ámbito de comunicación transnacional-universal, el ciberespacio, y porque sea en ese nuevo "lugar" en el que, desde cualquier espacio físico ubicado en cualquier Nación, se cometen infracciones que pueden afectar, en lugares distintos y simultáneamente, a bienes jurídicos tan diversos como el patrimonio, la intimidad, la libertad y la indemnidad sexuales, el honor, la dignidad persona, la seguridad del estado, la libre competencia entre otros muchos"*[14]

Desde este planteamiento, el concepto de *ciberdelito* puede ser doble[15]: una *perspectiva amplia* entendiendo por tal cualquier comportamiento delictivo realizado en el ciberespacio, esto es, el ámbito virtual de interacción y comunicación definido por el uso de las TIC´s, y abarcando tanto nuevas conductas ilícitas relacionadas directamente con los nuevos intereses o bienes existentes en el ciberespacio, como tipos delictivos tradicionales en los que cambia el modo de comisión que se realiza a través de las TIC´s; y un *concepto restringido*, de manera que la esencia del delito radica en que se realice de manera exclusiva mediante las nuevas tecnologías, con ello, sólo estaremos en presencia de un ciberdelito cuando se trate de un comportamiento que de ninguna manera se hubiera podido producir fuera del ciberespacio. Así, todos aquellos supuestos que pudieran realizarse al margen del ciberespacio, como por ejemplo, un delito contra la intimidad, no serían *ciberdelitos* en virtud del concepto restringido, aunque sí lo serían para el concepto amplio.

Sobre esta base, y dada la regulación que contiene nuestro Código penal de las figuras típicas realizadas mediante nuevas tecnologías, es preciso señalar que debe mantenerse una *concepción amplio* de manera que estará incluido cualquier comportamiento típico en el cual las TIC´s representen un papel determinante en su concreta comisión, o como igualmente señala MIRO LINARES[16], *"cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan*".

II. Los ciberdelitos en el código penal español tras la reforma del 2015

Tras las reformas efectuadas por las LLOO 5/2010, 1/2015 y 2/2015, son numerosos los delitos incluidos en el Código penal en los que las TIC´s constituyen bien los medios de comisión de los mismos, o bien operan como agravantes, así, por ejemplo, el *stalking* o acoso regula modalidades en las que se emplean las TIC´s, el descubrimiento o revelación de secretos, el *sexting*, las calumnias e injurias, el *grooming*, estafa informática, delitos contra la propiedad intelectual, los daños informáticos, delitos de odio o delitos de terrorismo, entre otros. Haremos referencia a algunos de ellos que han resultado más modificados o novedosos en las últimas reformas penales:

1. Estafa informática (art. 248.2 Cp)

En el Código penal de 1995 se incorpora una modalidad de estafa que en realidad difícilmente responde a

la estructura de la misma al faltar dos de los principales elementos, esto es, engaño y error, aunque sí están presentes el acto de disposición patrimonial y el perjuicio. Se trataba de la denominada estafa informática que consistía en aquellas conductas en las que mediante *alguna manipulación informática o artificio semejante se realizara una transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero*, figura que hoy se encuentra regulada en el art. 248.2 a) Cp. De este modo, la esencia principal consiste en la realización de un acto de disposición patrimonial y el consecuente perjuicio mediante la utilización de las TIC´S, siendo muy variados los medios de comisión de la misma. Así pueden diferenciarse varias técnicas de realización de estos comportamientos[17]:

a.- Obtención de datos o claves de acceso a determinados servicios y uso indebido de los mismos: se trata de las técnicas conocidas como *spyware, phising* y *pharming*[18], que esencialmente constituyen formas de acceder a las claves y datos de las víctimas para después emplearlas en el acceso a las cuentas bancarias o tarjetas de crédito de las víctimas.

b.- *Dialers* (conexiones telefónicas fraudulentas): consiste en el uso de programas de marcado telefónico que establecen una conexión telefónica a redes mediante un número de tarificación adicional de altísimo coste, y en las que no se informa adecuadamente o se oculta de modo específico las consecuencias de su instalación[19].

c.- Fraudes en operaciones de comercio electrónico: se refiere a supuestos en los cuales a través de las TIC`s se realizan operaciones comerciales que determina que los bienes adquiridos no se envíen o que se entreguen otros que no reúnen las características ofertadas.

d.- Envío de mails masivos: mediante los cuales se pueden realizar diversos tipos de fraudes, enviando a las víctimas diversas ofertas (trabajo, negocios fáciles, comunicaciones de cargos de tarjetas de crédito por operaciones nunca efectuadas, etc.) donde los gastos de tramitación de la oferta falsa o de comunicación para solventar el problema que nunca existió son los que ocasionan el perjuicio patrimonial.

Junto a esta modalidad específica de estafa informática prevista en el apartado a) del art. 248.2, sucesivas reformas penales han ido incorporando nuevas modalidades directamente relacionadas con la utilización de las TIC´s. Así, en el apartado b) se sanciona una supuesto de actos preparatorios del delito de estafa (eso sí, con la misma pena que la estafa consumada), incriminando a quienes *fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo*. Del mismo modo, tras la reforma de 2010, se incluye un apartado c) donde se sanciona la *utilización de tarjetas de crédito o débito o los datos obrantes en las mismas para realizar operaciones de cualquier clase en perjuicio de su titular o de un tercero*, con los consiguientes problemas concursales con el robo con fuerza en las cosas, y la falsificación de determinados medios de pago del art. 399 *bis*.

*2. El **stalking o acoso***

La reforma de 2015 introduce una nueva figura delictiva entre los delitos de coacciones en el art. 172 *ter* mediante la que se incrimina específicamente el acoso a otra persona que es llevado a cabo mediante diversas formas de comisión, entre ellas y de manera relevante, a través de tecnologías de la información y la comunicación. Así, expresamente y aunque ello no obsta a que el resto de las modalidades también sean realizadas mediante las TIC´s, el nº 2º del precepto establece específicamente, la constitutiva de ciberdelito, de manera que el autor debe establecer el contacto con la víctima mediante un medio de comunicación. Sería el caso de uso de redes sociales en Internet o aplicaciones informáticas instaladas en un teléfono móvil como es el caso de Whatsapp que permite enviar mensajes de texto o imágenes de forma instantánea a cualquier número de móvil.

3. Descubrimiento y revelación de secretos

Las reformas del Código penal en esta materia han determinado la incorporación como conductas típicas de comportamientos consistentes en *hacking, Black Hacking* **y demás técnicas de acceso no consentido, estableciendo no sólo modalidades expresas en el delito de descubrimiento y revelación de secretos previsto en el art. 197 Cp en las que se emplean medios o modos tecnológicos, como el denominado** *robo de identidad*[20] **(art. 197.2), sino mediante la expresa tipificación del** *intrusismo informático o acceso inconsentido* **a un sistema de información, en el art. 197** *bis***, así como la creación o posesión de programas informáticos o contraseñas o códigos de acceso que permitan realizar ese intrusismo, en el art. 197** *ter*.

Del mismo modo, la reforma del 2015 incluye el denominado *sexting* en el número 7 del art. 197, mediante el que se sancionan los supuestos en los que se produzca una *difusión no autorizada de imágenes o grabaciones audiovisuales obtenidas con consentimiento*, siempre que hayan sido realizadas en un contexto de intimidad.

IV. Grooming[21]

De manera similar a los supuestos de acoso que hemos analizado, se trata de un *ciberacoso* con finalidad sexual realizado contra los menores de 16 años, y que se encuentra previsto en el art. 183 *ter*. Así se trata de acciones realizadas por un adulto, utilizando para ellos medios tecnológicos virtuales (Internet, Salas de Chat, redes sociales, etc.), teléfono o cualquier otra tecnología de la información o la comunicación, con el objetivo de concertar un encuentro con el menor con la finalidad de cometer un delito sexual. En el número segundo del art. 183 *ter*, se sancionan los actos dirigidos a embaucar a un menor de 18 años a fin de que, mediante esos mismos medios tecnológicos, facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor.

V. Daños informáticos

También se incluyen dentro de los *ciberdelitos* más importantes el de los daños informáticos, realizados de manera general por los denominados *crackers*[22], quienes específicamente cometen daños en los sistemas informáticos mediante el acceso o la infección de estos. De manera intencional los *crackers* violan la seguridad de un sistema informático para hacerle daño, eliminar o borrar ficheros, así como introducir algún tipo de virus en él.

Esta será la figura típica prevista en los arts. 264, 264 *bis* y 284 *ter* del Código Penal. Sobre esta base, los sujetos activos pueden realizar dos tipos de conductas esencialmente: el bloqueo o inutilización, ya sea parcial o total, temporal o definitivo, de páginas web o servicios de Internet, y la destrucción o alteración, total o parcial de contenidos, información o datos ajenos. Para ello son numerosas las formas de comisión que pueden emplear: así, la eliminación informática de archivos, la introducción en el sistema de virus, gusanos, bombas lógicas, troyanos, bacterias o puertas traseras[23], y, una de las modalidades más llamativas, cual es la denegación de servicio que consiste en acciones encaminadas al bloqueo de los equipos mediante el envío de mensajes falsos o gran cantidad de información provocando su colapso y haciendo caer al sistema. No obstante el delito solo quedará constituido cuando la inutilización sea total, no una simple alteración en su funcionamiento.

VI. Otros tipos penales directamente relacionados con el empleo de las TIC´s

Son muchos los tipos penales respecto de los cuales existe algún tipo de vinculación con las nuevas tecnologías, por ejemplo, los *relativos a la propiedad intelectual* que, al margen de la propia problemática que pudiera determinar la utilización de estos medios como forma de atentar contra el bien jurídico como, por ejemplo, los casos de piratería informática de los arts. 270 y ss. del Código penal, también se ha incorporado expresamente al Código penal, la sanción de la facilitación del acceso a la localización en internet de las obras o prestaciones objeto de propiedad intelectual (lo que se conoce como páginas de enlaces[24]), en el apartado 2 del art. 270, así como la fabricación, comercialización o venta de cualquier medio concebido para facilitar la supresión o neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquier otra obra.

También es necesario hacer referencia dentro de los ciberdelitos a lo que se ha denominado *ciberterrorismo* y a los delitos de odio a través de redes sociales. Por lo que se refiere al primero de ellos, esto es el ciberterrorismo, son distintos los ámbitos en los que las nuevas tecnologías determinan su influencia.

El *ciberterrorismo* ha sido considerado doctrinalmente, aunque no sea la naturaleza propiamente de terrorismo como tal, como una modalidad en las conductas son realizadas por medio de la red o a través de cualquier tecnología de la información y la comunicación, siempre y cuando conlleven alguna de las finalidad expresamente previstas por el art. 573.1[25]. De este modo, de forma expresa se califican como delitos de terrorismo en el art. 573.2, los delitos informáticos tipificados en los arts. 197 *bis* y 197 *ter,* así como los de los arts. 264 a 264 *quater* cuando se comentan con alguna de las finalidades previstas en el número anterior, es decir, los casos de ataques masivos a los sistemas informáticos o simplemente los accesos ilícitos a los mismos, con alguna de las finalidades "terroristas" enumeradas. De este modo, los ataques a la intimidad o daños informáticos que sean realizados, por ejemplo, de obligar a un poder público a abstenerse de realizar un acto en concreto, como pudiera ser llevar a cabo el lanzamiento en un desahucio (por ejemplo, inutilizando el ordenador del Juzgado para impedir que se dicte la resolución al efecto), podría llegar a constituir un delito de terrorismo (recordemos que tras la reforma de la LO 2/2015, el elemento estructural ya no resulta necesario, con lo cual podría cometerse por un autor individual). Se comenta por sí mismo.

Pero no terminan aquí los supuestos que pudieran considerarse como ciberterrorismo, otro claro ejemplo de la influencia de las TIC´s en estos delitos lo constituye el denominado *autoadiestramiento o autocapa-*

citación contenido en el art. 575 Cp, de manera que se sanciona penalmente a quien con la finalidad de adiestrarse o capacitarse para la comisión de delitos de terrorismo, *acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de Internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines.* De este modo, se sanciona a quien accede, esto es, al usuario particular, a diferentes contenidos on line donde organizaciones terroristas incorporan contenidos relativos a su ideología y métodos que incitan a que los usuarios se unan a su red. En mi opinión, la lesión de la libertad individual resulta innegable, todo ello en aras de "combatir" presuntamente el terrorismo desde estadios que ni siquiera son tales todavía.

Una tercera cuestión en materia de terrorismo mediante el empleo de las nuevas tecnologías, se recoge en el art. 578. 2 que recoge un tipo cualificado del delito de enaltecimiento o justificación del terrorismo, cuando los *hechos se hubieran llevado a cabo mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, Internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información. Añadiendo el número 4 del mismo precepto que para* este caso*, el juez o tribunal podrá ordenar la retirada de los contenidos o servicios ilícitos. Subsidiariamente, podrá ordenar a los prestadores de servicios de alojamiento que retiren los contenidos ilícitos, a los motores de búsqueda que supriman los enlaces que apunten a ellos y a los proveedores de servicios de comunicaciones electrónicas que impidan el acceso a los contenidos o servicios ilícitos (...).* Similar regulación se ha previsto en relación con los delitos de odio, al establecer el art. 510. 3 un tipo cualificado cuando se realicen las conductas a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información.

Bibliografía

Colás Turégano, "El delito de intrusismo informático tras la reforma del CP español de 2015", en Revista Boliviana de Derecho, nº 21, Enero 2016.

Fernández Teruelo, Cibercrimen. Los delitos cometidos a través de internet, Constitutio Criminalis Carolina, 2007.

Galán Muñoz, "Ataques contra sistemas informáticos", en La armonización del Derecho Penal español: una evaluación legislativa, Boletín del Ministerio de Justicia, año 60, nº extra 2015, 2006.

Galán Muñoz, "El robo de identidad: aproximación a la nueva y difusa figura delictiva", en Robo de identidad y protección de datos, Aranzadi, 2010.

Galán Muñoz, "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", en Revista Penal, nº 24, Julio 2009.

Galán Muñoz, El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 Cp, Valencia 2005.

Galán Muñoz. "¿Nuevos riesgo, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y de la comunicación", en La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación, Galán Muñoz (coord.), Valencia 2014.

González Rus, "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en Poder Judicial, nº Especial IX, 1989.

Mata y Martín, Delincuencia informática y Derecho Penal, Madrid 2001.

Mendoza Calderón, El Derecho penal frente a las formas de acoso a menores. Bullying, ciberbullying, grooming y sexting, Valencia 2014.

Miro Linares, "La oportunidad criminal en el ciberespacio", en RECPC 13-07 (2011).

Miro Linares, El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Marcial Pons, 2012.

Morón Lerma, E., Internet y Derecho penal: Hacking y otras conductas ilícitas en la red, Aranzadi, Pamplona, 1999.

Notas

1 Cfrs. GALÁN MUÑOZ, "La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales", en *Revista Penal*, nº 24, Julio 2009, p. 90.

2 Cfrs. COLÁS TURÉGANO, "El delito de intrusismo informático tras la reforma del CP español de 2015", en *Revista Boliviana de Derecho*, nº 21, Enero 2016, p. 212.

3 Tal como señala MIRO LINARES, *El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, 2012, p. 26, el término *ciberespacio* fue acuñado por William Gibson, interpretando por tal un espacio comunicativo e interactivo que, de forma paralela al mundo físico, ha modificado las relaciones económicas, políticas, sociales y, muy especialmente, las personales.

4 Así, los servicios de Internet o la telefonía móvil son los vehículos por los que fluye la mayor parte del dinero en el mundo, de manera que prácticamente todos los bancos y entidades financieras actúan a través del *ciberespacio*.

5 Cfrs., MIRO LINARES, *El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, 2012, p. 26.

6 Así, MIRO LINARES, *El cibercrimen*, op. cit., p. 27, afirma que *"la evolución de cibercrimen como fenómeno criminológico ha transcurrido de forma paralela (…)a la evolución de los intereses sociales relacionados con las TIC: cuando el protagonismo lo tuvieron las terminales informáticas y la información personal que ellas podían contener, aparecieron nuevas formas de afectar a la intimidad de las personas; cuando dichas terminales y la información en ellas contenida comenzaron a tener valor económico y a servir para la realización de transacciones económicas, surgieron las distintas formas de criminalidad económica relacionadas con los ordenadores y muy especialmente el fraude informático que, a su vez, evolucionó hacia el* scam*, el* phishing*, y el* pharming *cuando apareció internet; finalmente, con la universalización de la Red y la constitución del ciberespacio comenzaron a surgir nuevas formas de criminalidad que aprovechaban la transnacionalidad de Internet para atacar intereses patrimoniales y personales de usuarios concretos, pero también para afectar intereses colectivos por medio del ciberracismo o del ciberterrorismo".*

7 Cfrs. MIRO LINARES, *El cibercrimen, ibidem.*

8 Cfrs. COLAS TURÉGANO, "El delito de intrusismo informático", op. cit., p. 213.

9 Así pueden señalarse el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest de 23 de noviembre de 2001, la Decisión Marcos 2004/68/JAI del Consejo, de 22 de diciembre de 2003 relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero, relativa a los ataques contra los sistemas de información, y la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto relativa a los ataques contra los sistemas de información.

10 Cfrs. GALÁN MUÑOZ, "La internacionalización de la represión y la persecución de la criminalidad informática…", op. cit., p. 92.

11 Cfrs. GALÁN MUÑOZ, "La internacionalización de la represión y la persecución de la criminalidad informática…", op. cit., p. 93.

12 Así, señala MIRO LINARES, "La oportunidad criminal en el ciberespacio", en *RECPC* 13-07 (2011), p. 07:3, que la denominación delitos informáticos o *computercrimes* expresaba perfectamente la preocupación por un tipo de delincuencia surgida con la aparición de los primeros sistemas informáticos, en la que éstos eran el medio o el objetivo del crimen; de este modo, implicaba que se encontraban insertos en dicha denominación tanto los comportamientos delictivos realizados a través de procesos electrónicos, como aquellos otros delitos tradicionales que recaían sobre bienes que presentaban una configuración específica en la actividad informática, o bien sobre nuevos objetos como el *hardware* y el *software*, y al mismo tiempo que no definieran un bien jurídico protegido común a todos ellos, sino más bien un ámbito de riesgo que se derivaba de la expansión social de la tecnología informática, cfrs. MIRO LINARES, *El cibercrimen*, op. cit., pp. 35 y 36. En este mismo sentido, MATA Y MARTÍN, *Delincuencia informática y Derecho Penal*, Madrid 2001, p. 23 y ss; GONZÁLEZ RUS, "Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", en *Poder Judicial*, nº. Especial IX, 1989, pp. 40 y ss. Este ámbito de riesgo afectaba a todo tipo de bienes jurídicos e intereses, y así se hacía referencia al fraude informático, los daños informáticos, el *hacking* o acceso ilícito a sistemas informáticos, el espionaje informático o la piratería informática, entre otros.

13 Con ello se hace referencia al término anglosajón *cybercrime*, cfrs. MIRO LINARES, "La oportunidad criminal en el ciberespacio", op. cit., p. 07:2.

14 Cfrs. MIRO LINARES, "La oportunidad criminal en el ciberespacio", op. cit., p. 07:3.

15 En relación con esta clasificación seguimos el planteamiento de MIRO LINARES, *El cibercrimen*, op. cit., pp. 42 y 43.

16 Cfrs. MIRO LINARES, *El cibercrimen*, op. cit., p. 44.

17 En relación con la estafa informática, véase GALÁN MUÑOZ, *El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 Cp*, Valencia 2005.

18 Así el *spyware* implica que se instale un archivo espía en el ordenador del sujeto pasivo, que envía información al autor sobre el sistema o las claves de acceso; el *phising* que consiste en el envío de correos electrónicos a la víctima a través de los cuales el titular de los datos facilita contraseñas o números de cuentas corrientes o tarjetas de crédito por creer que se los estaba dando a la entidad que se los había suministrado para identificarle; y el *pharming* consiste en comportamientos en los que el autor modifica las direcciones web para reconducir a la víctima a páginas falsas en las que proporciona su información personal en el convencimiento de que se encuentra en páginas reales, cfrs. GALÁN MUÑOZ. "¿Nuevos riesgo, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y de la comunicación", en *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Galán Muñoz (coord.), Valencia 2014, nota 70, p. 234.

19 Cfrs. FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de internet*, Constitutio Criminalis Carolina, 2007, p. 32.

20 Cfrs. GALÁN MUÑOZ, "¿Nuevos riesgos, viejas respuestas'", op. cit., pp. 208 y ss.; el mismo, "El robo de identidad: aproximación a la nueva y difusa figura delictiva", en *Robo de identidad y protección de datos*, Aranzadi, 2010, pp. 169 y ss.

21 Cfrs. MENDOZA CALDERON, *El Derecho penal frente a las formas de acoso a menores. Bullying, ciberbullying, grooming y sexting*, Valencia 2014, pp. 94 y ss.

22 Cfrs. MORÓN LERMA, E., *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red,* Aranzadi, Pamplona, 1999, pp. 32-33. Para la autora el *cracking* difiere de una conducta análoga para muchos, el *cyberpunk,* siendo esta última una mezcla entre el *hacker* y el *cracker*, pues consiste en la entrada inconsentida en sistemas informáticos (*hacking)*, pero mediando la corrupción de un *password* (*cracking),* para provocar la destrucción de datos, programas o soportes informáticos, o introducir un virus, una bomba lógica o algo similar. Son conductas similares que comprenden el llamado "vandalismo electrónico" o *ciberpunk*, refiriéndose exclusivamente al daño en Internet y que también encuentran cabida en el art. 264 CP. Se vincula a la defraudación de la propiedad intelectual, ya que al dañar el sistema se consigue evitar la protección de los programas informáticos.

23 Mediante esta conducta delictiva se introducen programas informáticos específicos en el sistema informático que le va destruyendo, tanto a él como a los programas y ficheros que contiene, a la vez que se va propagando a otros sistemas. Se consigue el acceso directo o a distancia al sistema, logrando la destrucción o el daño del mismo. Cfrs. GALÁN MUÑOZ, "Ataques contra sistemas informáticos", en *La armonización del Derecho Penal español: una evaluación legislativa*, Boletín del Ministerio de Justicia, año 60, nº extra 2015, 2006, pp. 225 y ss.; FERNÁNDEZ TERUELO, J., G., *Cibercrimen, los delitos cometidos a través de Internet,* op. cit., p. 110-111.

24 Estas son páginas webs que directamente no realizan ninguna conducta punible, pues ellas no reproducen, plagian, distribuyen o comunican públicamente obras protegidas, se trata de los comportamientos de páginas que contienen enlaces ordenados y clasificados, con información de su contenido y que conducen al usuario de manera sencilla e interactiva hacia terceras páginas en que se realizan los comportamientos del tipo básico del art. 270.1 CP.

25 En este punto resulta necesario poner de relieve la desmesurada ampliación que la LO 2/2015 realizó respecto de estas finalidades, determinando con ello, junto con la eliminación del elemento estructural como imprescindible para la realización de los delitos terroristas, una absoluta desvirtuación de lo que por terrorismo se entendía hasta el momento, incluyendo en este concepto supuestos que poco o nada tienen que ver con el terrorismo tradicional.

Honduras

Dra. Angie Andrea Arce Acuña
Doctora en Derecho, Costa Rica

I. Introducción

La humanidad se ha visto inmersa en una serie de cambios, que la han llevado a un desarrollo jamás pensado por nuestros antepasados, el internet, la computadora, la fibra óptica y la Globalización, corresponden a un nuevo modelo de desarrollo que genera cambios en cada país. Sin embargo con esos cambios, también vienen nuevas formas de delincuencia que debe ser tutelada. La sociedad se encuentra en un momento histórico que requiere de una tutela especializada en el caso de bienes jurídicos que anteriormente no eran puestos en peligro o lesionados, pero que con el advenimiento de los medios tecnológicos se hace necesario una tutela. Es el caso de los llamados delitos informáticos o ciber delincuencia.

Se puede definir como delito informático como *"crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de pcs o del Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.*

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datacredito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros".[1]

Los actos ilegales realizados a partir de la tecnología, no se habían tipificado como delitos en la mayoría de legislaciones; empero, el avance de un campo tan basto como el de la informática, si por un lado ha permitido el crecimiento tecnológico y económico de la sociedad, por otro lado, paradójicamente, ha venido a significar el instrumento idóneo para menoscabar el patrimonio económico de personas e instituciones. Quizá hasta hace poco no se consideraba necesario resguardar el bien jurídico de la información; sin embargo, actualmente es completamente evidente la relevancia de hacerlo ya que con estos delitos se ven comprometidos otros bienes jurídicos tutelados como el patrimonio o la protección de datos personales, entre muchos otros.

Es por esto que en aras de penalizar acciones y tutelar el bien jurídico de la información y generar herramientas eficientes y eficaces para condenar delitos

informáticos que afectan cada vez más el patrimonio de los costarricenses, se presenta el siguiente proyecto de ley.

II. Regulación en honduras

En el caso de Honduras, los medios que se han venido empleando para la tutela de este tipo de delitos se regulan en el Código Penal Hondureño mediante figuras genéricas como el caso del Capítulo IX, como Daños, los daños a los sistemas informáticos. Sin embargo no existe normativa especifica, de delitos informáticos que venga a tutelar las nuevas conductas, no hay una ley de delitos informáticos, tampoco a ratificado Tratados Internacionales que fomentan su protección como el Convenio de Budapest.

En Honduras los delitos informáticos implican actividades criminales encuadradas en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras como medio para delinquir ha propiciado la necesidad urgente de regular otras elementos relacionados por parte del derecho.

Actualmente existe en honduras un proyecto para un nuevo Código Penal, impulsado por el titular del Congreso Nacional, Mauricio Oliva, que contiene cincuenta nuevas figuras penales para tutela de la ciber delincuencia. La propuesta incorpora los delitos informáticos, fiscales, manipulación genética, graduación del homicidio, castigo para las pandillas que tengan controlados los negocios, delitos contra la economía, delitos financieros y delitos contra la propiedad.

El mencionado proyecto viene a sustituir las figuras genéricas que se venían utilizando para la tutela de nuevo código cambia el esquema de las estafas, incorporando fraudes por cheque, fraudes corporativos, delitos ambientales, corrupción pública, corrupción privada, conspiración y proposición de delitos en los que se pongan en riesgo o lesionen en mayor medida bienes jurídicos de mayor trascendencia.

Entre ellos esta el acceso e intercepción Ilícita Artículo 214 que indica "quien sin la debida autorización judicial, con cualquier propósito, se apodere de los papeles o correspondencia de otros, intercepta o hace interceptar sus comunicaciones telefónicas, telegráficas, soportes electrónicos o computadoras, facsimilares o de cualquier otra naturaleza, incluyendo las electrónicas, será sancionado con seis (6) a ocho (8) años si fuere un particular y de ocho (8) a doce (12) años si se tratare de un funcionario o empleado publico Atentado contra la seguridad de datos. Este tipo penal viene a tutelar la protección de datos, información y documentos.

Para la protección tanto del software como del hardware se tiene el artículo 254, que tutela "Se impondrá reclusión de tres (3) a cinco (5) años a quien destruya, inutilice, haga desaparecer o de cualquier modo, deteriore cosas muebles o inmuebles o animales de ajena pertenencia, siempre que el hecho no constituya un delito de los previstos en el capítulo siguiente. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos"

Una de las conductas delictivas mas importantes a tutelar se tiene la pornografía infantil Artículo 149-D, donde se indica que "Comete el delito de pornografía, quien por cualquier medio sea directo, mecánico o con soporte informático, electrónico o de otro tipo financie, produzca, reproduzca, distribuya, importe, exporte, ofrezca, comercialice, o difunda material donde se utilice la persona e imaginen de personas menores de dieciocho (18) años de edad en acciones o actividades pornográficas o eróticas, será sancionado con pena de diez (10) a quince (15) años de reclusión y multa de doscientos (200) a trescientos (300) salarios mínimos. La tenencia de material pornográfico de niños, niñas y adolescentes será sancionada con pena de cuatro (4) a seis (6) años de reclusión".

Mediante la Estafas por medios electrónicos, se introduce Artículo 241. "El delito de estafa será sancionado: 1) Con dos (2) a cinco (5) años de reclusión, cuando el valor de lo estafado no exceda de cinco mil lempiras (L. 5, 000.00); 2) Con cuatro (4) a siete (7) años de reclusión si la cuantía supera los cinco mil (L.5, 000.00) y no excede de cien mil lempiras (L. 100.000.00); y, 3) Con seis (6) a nueve (9) años de reclusión si la cuantía excede de cien mil lempiras (L. 100,000.00). El agente, además será sancionado con una multa igual al diez por ciento (10%) del valor defraudado. Lo anterior se entenderá sin perjuicio de lo prescrito por los artículos 36, 37 y 53, cuando sean aplicables. 117 Artículo 242. Incurrirá en las penas del artículo anterior:

14) Quien cometiere fraude en telecomunicaciones, medios u ondas y sistemas informáticos o de la información como tráfico irregular, a través de la reoriginación (refiling), reoriginación de llamada internacional (callback), ingreso de tráfico internacional de forma ilegal evitando pagar las debidas tasas de terminación entre operadores internacionales (bypass), piratería informática (hackeo), reventa no autorizada y clonación de números telefónicos móviles;

Otro de los artículos que vienen a integrar la protección contra la ciber delincuencia es el Artículo 394-I. "Utilización indebida de sistemas de procesamiento de datos. Quien acceda ilegalmente a los sistemas de procesamientos de datos de las instituciones supervisadas, para alterar, borrar, dañar o sustraer registros, archivos u otra información de la institución o de sus clientes en beneficio propio o ajeno, será sancionado con reclusión de tres (3) a seis (6) años cuando el monto de lo defraudado no exceda de diez mil (L 10, 000.00) lempiras y de seis (6) a doce (12) años cuando exceda de dicho monto. En las mismas penas incurrirán quienes bajo cualquier procedimiento ingrese o utilice indebidamente la base de datos de una institución supervisada para sustraer dinero mediante transferencias electrónicas de una cuenta a otra en la misma o diferente institución. Y quien utilice tarjeta de crédito o de debito de otra persona para hacer pagos de cualquier naturaleza, fingiéndose titular de la misma".

III. Estado actual de la ciberdelincuencia en honduras

El jefe del laboratorio de investigación de ESET-Latinoamérica, Camilo Gutiérrez, ha indicado que Honduras, no esta exenta y corre gran peligro cuando se trata de cyber delincuencia.

Gutiérrez señaló que "el cibercriminal se ha vuelto un lucrativo negocio, atacando muchos usuarios y así lograr que algunos de ellos paguen por recuperar la base de datos, dentro de otros delitos se tiene la pornografía infantil, que no únicamente debe darse una protección legal sino que cada usuario debe necesariamente tomar medidas preventivas para evitar que se de este tipo de delitos.

El tema de la Ciberdelincuenca informática es un tema sin duda de los más importantes, en la nueva sociedad informática porque encierra la tutela a derechos fundamentales como la intimidad, pero como lo afirmaron los juristas Warren y Brandeis, de paso sirve para lesionar otros derechos del ser humano.

En Honduras se toman las primeras armas para luchar contra los problemas que pudiera causar el uso de los datos de forma inadecuada en una persona, estafas, abuso infantil, la propuesta de reforma de Código Penal es la más importante de las reformas, ya que es generar en la conciencia de cada ciudadano respeto y cuidado hacia estos delitos, procurando hacer hombres y mujeres respetuosos de los derechos de las personas, que se entienda que no solo se debe respetar la vida humana, sino que además hay derecho muy importantes como los expuestos. Debe también hacerse campañas para informar a los ciudadanos del derecho que poseen y como protegerlo de tal manera tendrán más cuidado cuando vayan a trasmitir sus datos, y utilizar medios tecnológicos, de igual forma es importante la participación por parte del Estado a pertenecer a tratados internacionales que vayan contra la cyberdelicuencia asi como hacer leyes especificas encaminadas a la protección de este tipo de bienes jurídicos.

Notas

1 http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

México

Delitos informáticos. referencia al sistema jurídico mexicano

Manuel Vidaurri Aréchiga
Universidad De La Salle Bajío, México

El Título Noveno del **Código Penal Federal** (CPF) se compone de dos capítulos, el primero que se ocupa de la *revelación de secretos* y el segundo del *acceso ilícito a sistemas y equipos de informática*. El segundo capítulo fue introducido en el año 1999. El hecho de que tal adición haya sido en el apartado relacionado con la privacidad del individuo pretende, de algún modo, ampliar el ámbito de protección penal.

Conforme a lo anterior, tendría que considerarse de modo integral el contenido del Título Noveno a fin de comprender los alcances que el legislador contempló en su momento. De tal modo, dispone el artículo 210 del CPF como sanción la imposición de treinta a doscientas jornadas de trabajo en favor de la comunidad, "al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto". Para el supuesto de que la reveleción punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado publico o cuando el secreto revelado o publicado sea de carácter industrial, la sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año (artículo 211 del CPF).

Por otra parte, indica el artículo 211 bis, lo siguiente: "A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se

le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa". Este numeral, introduce o sirve de base para lo que se establece en el Capítulo II, del señalado Título Noveno, y que se ocupa precisamente del acceso ilícito a sistemas y equipos de informática. Textualmente, los artículos que se ocupan del tema prescriben lo siguiente:

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Aparte de las anteriores disposiciones legales del CPF, la Ley Federal de Derechos de Autor (LFDA) —publicada en el Diario Oficial de la Federación del 24 de diciembre de 1996—, en el Capítulo V, bajo la denominación *De los Programas de Computación y las Bases de Datos*, define aspectos de relevancia para el tema de este reporte. En tal sentido, se define lo que se entiende por programa de computación como la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica (artículo 101 LFDA). Por lo que respecta a la protección de los programas de cómputo, será en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos (artículo 102 LFDA).

Esta LFDA puntualiza (Artículo 106) que el derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;

II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;

III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y

IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

En otro apartado, se dispone en la LFDA que las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos (artículo 107). Puntualmente, señala la ley que se comenta que el acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate, aunque quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos (artículo 109). De modo expreso, se plasma en la LFDA (artículo 110) que el titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

El legislador dispuso una prohibición tajante, al tenor de lo que textualmente se transcribe ahora: "Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior" (artículo 112 LFDA).

Otras disposiciones complementarias pueden conocerse en diversos artículos contenidos en la **Ley de Propiedad Intelectual** (LPI) —Diario oficial de la Federación del 27 de junio de 1991— cuyo artículo 2, menciona que,entre otros objebivos, se encuentran los de "Promover y fomentar la actividad inventiva de aplicación industrial, las mejoras técnicas y la difusión de conocimientos tecnológicos dentro de los sectores productivos; Favorecer la creatividad para el diseño y la presentación de productos nuevos y útiles; Proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, marcas, y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales; así como Prevenir los actos que atenten contra la propiedad industrial o que constituyan competencia desleal relacionada con la misma y establecer las sanciones y penas respecto de ellos.

La citada LPI contiene un Capítulo dedicado a señalar que conductas son consideradas delictivas, de manera que (artículo 223 LPI) se consideran como tales las siguientes:

I. Reincidir en las conductas previstas en las fracciones II a XXII del artículo 213 de esta Ley, una vez que la primera sanción administrativa impuesta por esta razón haya quedado firme;

II. Falsificar, en forma dolosa y con fin de especulación comercial, marcas protegidas por esta Ley;

III. Producir, almacenar, transportar, introducir al país, distribuir o vender, en forma dolosa y con fin de especulación comercial, objetos que ostenten falsificaciones de marcas protegidas por esta Ley, así como aportar o proveer de cualquier forma, a sabiendas, materias primas o insumos destinados a la producción de objetos que ostenten falsificaciones de marcas protegidas por esta Ley;

IV. Revelar a un tercero un secreto industrial, que se conozca con motivo de su trabajo, puesto, cargo, desempeño de su profesión, relación de negocios o en virtud del otorgamiento de una licencia para su uso, sin consentimiento de la persona que guarde el secreto industrial, habiendo sido prevenido de su confidencialidad, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto;

V. Apoderarse de un secreto industrial sin derecho y sin consentimiento de la persona que lo guarde o de su usuario autorizado, para usarlo o revelarlo a un tercero, con el propósito de obtener un beneficio económico para sí o para el tercero o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o a su usuario autorizado, y

VI. Usar la información contenida en un secreto industrial, que conozca por virtud de su trabajo, cargo o puesto, ejercicio de su profesión o relación de negocios, sin consentimiento de quien lo guarde o de su usuario autorizado, o que le haya sido revelado por un tercero, a sabiendas que éste no contaba para ello con el consentimiento de la persona que guarde el secreto industrial o su usuario autorizado, con el propósito de obtener un beneficio económico o con el fin de causar un perjuicio a la persona que guarde el secreto industrial o su usuario autorizado.

Los delitos previstos en este artículo se perseguirán por querella de parte ofendida.

Nicaragua

Sergio J. Cuarezma Terán
Profesor de Derecho penal
Instituto de Estudio e Investigación Jurídica (INEJ), sede Nicaragua

El Código penal nicaragüense (vigente desde 2008) no regula de forma específica los delitos informáticos (*cybercrimes*)", sino que contempla uno que otro tipo penal de forma aislada o fragmentada en el Código o bien, como modalidades periféricas de algún tipo penal.

En el título III, de los delitos contra la vida privada y la inviolabilidad del domicilio, capítulo I, delitos contra la vida privada, se regula la *apertura o interceptación ilegal de comunicaciones* (art 192), penado con prisión de seis meses a dos años; *captación indebida de comunicaciones ajenas* (art. 194), será penado con prisión de uno a dos años; *registros prohibidos* (art. 197), "el que sin autorización de ley promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que puedan afectar a las personas naturales o jurídicas", será penado con prisión de dos a cuatro años y de trescientos a quinientos días multa. También el *acceso y uso no autorizado de información* (art. 198), "quien, sin la debida autorización, utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco de datos o archivos electrónicos", se castigará con prisión de uno a dos años, y de doscientos a quinientos días multa.

En el titulo VI de los delitos contra el patrimonio y el orden socioeconómico, capítulo VIII, de los daños, se contempla la *destrucción de registros informáticos*, "quien destruya, borre o de cualquier modo inutilice registros informáticos", será penado con prisión de uno a dos años o de noventa a trescientos días multa. Esta pena se elevará de tres a cinco años, cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial (art. 245). En el artículo 246 regula el *uso de programas destructivos,* estableciendo "quien, con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación", será penado con[1] prisión de uno a tres años y de trescientos a quinientos días multa.

Notas

1 sergio.cuarezma@inej.net / www.sergiocuarezma.com

Panamá

Carlos Enrique Muñoz Pope
Catedrático de Derecho Penal
Universidad de Panamá
carlos.muñozpope@cableonda.net

I. Introducción

El Código Penal panameño de 2007 se ocupa, bajo la denominación "Delitos contra la seguridad jurídica

de los medios electrónicos" en el Título VIII del Libro Segundo, en un solo Capítulo (artículos 289 y 290) de algunas figuras delictivas que guardan relación con delitos usualmente conocidos como "delitos informáticos". En los arts. 291 y 292, por otra parte, se introducen circunstancias agravantes para los dos anteriores.

A pesar de lo antes expresado, sin embargo, es necesario destacar que en el resto del Libro Segundo se incorporan, en ocasiones muy puntuales, distintas formas de agravantes específicas para ciertos delitos en los que la utilización de medios tecnológicos, sistemas informáticos o base de datos permite o facilita la comisión de esos delitos.

Relativo a normas de seguridad informática, lo que persiguen castigar es el "acceso no autorizado", tutelando así el derecho a la intimidad frente a las conductas de "intruismo o hacking", más que tutelar el patrimonio o la seguridad colectiva frente a las numerosas conductas que mediante medios informáticos puedan afectar diversos bienes jurídicos como por ejemplo el fraude electrónico, el sabotaje informático.

De tales circunstancias, sin embargo, nos ocuparemos luego de examinar los artículos antes mencionados.

II. Los delitos bajo estudio en particular

El artículo 289 incrimina la conducta de quien "indebidamente ingrese o utilice una base de datos, red o sistema informático" con una pena de 2 a 4 años de prisión, lo cual responde a la conducta del llamado" "intruismo" informático (hacking).

Como se observa, estamos en presencia de un típico delito de "peligro", ya que no se requiere que el sujeto que ingresa o utiliza a la base de datos, red o sistema informático haya causado un daño al mismo o se haya aprovechado para obtener algún beneficio a su favor o en favor de un tercero, pues lo único que busca la norma es el respeto al bien jurídico "Seguridad Informática", aunque se pueda considerar de carácter pluriofensivo dependiendo de los medios empleados y quienes resulten afectados.

Por su parte el art. 290 incrimina a quien "indebidamente se apodere, copie, utilice o modifique los datos en tránsito contenidos en una base de datos o sistema informático o interfiera, intercepte, obstaculice o impida su transmisión" y tales conductas se castigan con pena de 2 a 4 años de prisión, conducta conocida como "cracking".

La cuestión central de esta norma, parece estar dirigida a impedir que se afecte la existencia e integridad de la información "en tránsito" de cualquier manera, lo que supone una conducta muy cercana a los delitos que afectan intereses bancarios, comerciales, secretos financieros y hasta la inviolabilidad del secreto. Ninguna de estas conductas requiere que se cause perjuicio alguno, aunque es evidente que modificar, obstaculizar o impedir la transmisión de datos en tránsito puede, efectivamente, perjudicas intereses particulares.

III. Las agravantes

En los artículos 291 y 292, como ya se indicó anteriormente, se incorporan diversas agravantes para los delitos 290 y 291 ya analizados.

Por tal razón, la pena se agravará de una sexta a una tercera parte si el delito se comete en una oficina pública o bajo la "tutela" del infractor; en instituciones públicas, privadas o mixtas que presten un servicio público y, finalmente, en bancos, aseguradoras o instituciones financieras o bursátiles.

La misma pena agravada se impondrá al encargado o responsable de la base de datos o sistema informático, al responsable de acceder al sistema o a quien realizó tales actos en virtud de información privilegiada.

Expresamente se dispone en el capítulo bajo análisis, que estas penas se impondrán concurrentemente si los hechos cometidos recaen sobre información confidencial que afecte la Seguridad del Estado.

IV. Otras situaciones puntuales

| Es frecuente encontrar referencias en otras figuras delictivas a delitos cometidos haciendo uso de medios tecnológicos o informativos para agravar penas en delitos de inviolabilidad del secreto y derecho a la intimidad (art. 164, 165, 166 y 167) corrupción de menores (arts. 184 y 187), delitos contra el honor (art. 195), hurto (art. 214), estafa (arts. 220 y 226), daños (art. 230), delitos financieros (art. 243), contra los derechos de autor y derechos conexos (arts. 264 y 265), "contra la seguridad colectiva (art. 295 y 295-A), revelación de secretos empresariales (art. 288) y falsedad (art. 366-A), del Código Penal panameño.

En tales delitos agravados, la agravante se aprecia por realizar el ilícito a través de internet, correo electrónico, sistema informático, medios tecnológicos, medios cibernéticos, mediante procesos automatizados entre otras expresiones).

V. Consideraciones finales

En lo que refiere a la tipificación de los delitos informáticos en Panamá, es necesario reformular el sistema

utilizado dentro del Código Penal para su tipificación, pues solo se centran en los delitos referidos al acceso indebido a un sistema informático, cuando ya es necesario hacer una reforma integral para adaptarlos a la normativa internacional vigente en muchos Estados modernos.

El tema tiene enorme trascendencia real y verdadera, pues las modernas tecnología controlan nuestro diario vivir. Un caso particular, por ejemplo, sería afectar el sistema informático del Canal de Panamá o de las empresas de servicio público en Panamá, que se manejan desde una amplia red de ordenadores que requieren operar bajo reglas de seguridad.

Es preciso destacar que las modernas conductas criminales en esta materia requieren de una amplia regulación, pues hasta el momento muchas de ellas solo aparecen tipificadas de forma genérica y tangencial en algunas de las agravantes antes mencionadas. Es el caso, por ejemplo, del "phishing", "carding" y "hoaxes" entre otros.

Nuestra doctrina poco ha dicho a este respecto. La tesis de maestría de Campo Elías Muñoz Arango sobre seguridad informática es un aporto serio para una eventual reforma sobre el particular.

Perú

Prof. Dr. Víctor Roberto Prado Saldarriaga
Catedrático de Derecho Penal
Juez Supremo Titular de la Corte Suprema de Justicia

I. El Actual Panorama Internacional

Recientemente tuvo lugar en Viena, entre el 10 y el 13 de abril de 2017, la Tercera Reunión Plenaria del "Grupo de Expertos encargado de realizar un Estudio exhaustivo sobre el Delito Cibernético" de las Naciones Unidas,. Por primera vez el Perú participó técnicamente en este importante espacio de reflexión y discusión comparativa sobre los esfuerzos de la comunidad internacional y de los Estados Miembros de la ONU para la prevención y control penal de tan relevante y sofisticada modalidad de criminalidad contemporánea.

Lamentablemente, el debate sobre la problemática actual de la Ciberdelincuencia se desgastó en torno a un marcado discenso sobre la utilidad presente del Convenio de Budapest del 2001 como estándar internacional para la criminalización y cooperación judicial internacional en materia penal. En ese contexto las delegaciones de China, Rusia y Brasil demandaron la necesidad de construir un Convenio Universal sobre la materia, aduciendo, sobre todo, que el instrumento de Budapest tenía origen regional y no había sido discutido ni aprobado por otros Estados ajenos al sistema europeo. Frente a ello las delegaciones de los Estados Europeos y de los Estados Unidos, con apoyo expreso de un importante núcleo de países americanos y africanos, sostuvieron la relevancia y universalización práctica del texto aprobado el 2001, así como de los documentos y estudios complementarios a él, especialmente del "Estudio Exhaustivo sobre el Delito Cibernético" elaborado por la Oficina de las Naciones Unidas contra la Droga y el Delito – UNODC, cuyo borrador se hizo público en febrero de 2013.

No obstante, quedó de manifiesto en dicha reunión internacional que aún subsisten importantes problemas y desafíos que afectan la eficacia de los sistemas nacionales o hemisféricos para interdictar y reprimir las distintas manifestaciones de los delitos informáticos. Destacando al respecto las limitaciones de los mecanismos de asistencia judicial mutua, los desniveles tecnológicos de los organismos de persecución y sanción del delito, así como las diferentes perspectivas aún predominantes sobre las fuentes, captación y valoración de las pruebas electrónicas.

En consecuencia, pues, si bien se ha avanzado de modo notable en los procesos de armonización legislativa en torno a la criminalización primaria de los ciberdelitos, las prácticas operativas para su detección oportuna en la amplitud del ciberespacio o de su evaluación criminalística eficiente adolecen todavía de marcadas debilidades. Por tanto, este debe ser el escenario de las acciones futuras para optimizar la actuación multinacional contra toda expresión de criminalidad informática organizada de operatividad convencional como la distribución de pornografía infantil o de marcada sofisticación como las complejas modalidades del ciberespionaje o sabotaje informático

II. La situación de la Cibercriminalidad en el Perú

La presencia actual de la delincuencia informática en el Perú es todavía moderada, básica y de visibilidad precaria. En efecto, la trascendencia de esta modalidad criminal no se hace sentir aún en las tipologías y estadísticas oficiales que a ella se refieren. Es así que en los dos últimos años sólo se registró un total de 2,290 casos de delitos cibernéticos intervenidos por la División de Investigación de Delitos de Alta Tecnología de la Dirección de Investigación Criminal de la Policía Nacional del Perú.

Ahora bien, de ese escaso volumen de delitos sometidos a pesquisa policial, 1294 casos correspondieron a

actos de fraude informático; 342 a prácticas de distribución y acceso a pornografía infantil; y 269 a modalidades de suplantación de identidad. Son pues, estos indicadores cuantitativos y cualitativos los que representan más del 80% de la criminalidad en línea que se registra en el país. No cabe duda, pues, que tales datos sólo muestran la punta del *iceberg* de una cifra negra mayor, la cual se ve favorecida por la amplia presencia de la informalidad informática en nuestra sociedad, así como por la todavía rudimentaria tecnología y capacidad operativa con la que cuenta la unidad policial especializada en estos hechos punibles. Pero, además, por la carencia de recursos humanos capacitados y de órganos expertos en la investigación o juzgamiento de los cibercrímenes en el Ministerio Público y en el Poder Judicial.

Asimismo, en el plano de la prevención, los avances estatales sobre gobierno digital, así como los programas diseñados para el fortalecimiento de la conectividad formal y el mejor acceso a servicios de internet en las localidades del interior nacional, no han diseñado aún un plan estratégico de alertas o de difusión masiva de los riegos y amenazas que se derivan del uso de los distintos servicios cibernéticos que se entrecruzan en nuestra realidad virtual. Por ejemplo, recientemente ha incursionado en el ámbito escolar la práctica de modalidades de instigación a las autolesiones y el suicidio, conocidas como "ballena azul".

III. El Marco Legal Vigente

El Código Penal de 1991 no incluyó en su texto original referencia alguna a delitos informáticos. Sólo con posterioridad el legislador nacional incorporó modalidades de realización de delitos patrimoniales, de violación del secreto de las comunicaciones y de afectación de derechos intelectuales a través de sistemas informáticos.

Recién en el año 2013, la legislación peruana se inserta en procesos de criminalización más técnicos y mejor elaborados con la promulgación de la Ley 30096 del 27 de setiembre de aquel año, a la que con logrado sentido ideográfico se denominó "Ley de Delitos Informáticos". Cabe señalar que esta disposición legal fue el resultado del debate de un conjunto de propuestas legislativas que revisó la Comisión de Justicia y Derechos Humanos del Congreso de la República, durante el periodo de sesiones 2011-2012. Al respecto, es ilustrativo sobre su objetivo político criminal de dar autonomía punitiva a esta clase de hechos punibles, el siguiente pasaje del Dictamen que elaboró la citada Comisión Parlamentaria: "Leyes especiales deben ser aprobadas en razón de que el ciberespacio es un ámbito relativamente nuevo de acción privada y pública, dónde los perpetradores de crímenes puedan gozar de mayores facilidades para eludir la persecución policial y judicial. Por ello los clásicos delitos señalados en el Código Penal no se pueden aplicar con la precisión que demanda el derecho penal. Por tanto, regular las implicancias que tiene la informática en el fenómeno delictivo resulta una cuestión actual y necesaria para quienes observan el impacto de las nuevas tecnologías en el ámbito social y jurídico" (Dictamen de la Comisión de Justicia y Derechos Humanos recaído en los proyectos de Ley 034/2011-CR, 307/2011-CR y 1136/2011-CR del 20 de julio de 2012, p. 3).

Por su parte, el artículo 1° de la Ley 30096 también destacaba como su principal objetico el de "prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia".

Al interior de la norma legal citada se regulaban las siguientes cinco tipologías delictivas:

- Delitos contra Datos y Sistemas Informáticos (Capítulo II).
- Delitos Informáticos contra la Indemnidad y Libertad Sexuales (Capítulo III).
- Delitos informáticos contra la Intimidad y el Secreto de las Comunicaciones (Capítulo IV).
- Delitos Informáticos contra el Patrimonio (Capítulo V).
- Delitos Informáticos contra la Fe Pública (Capítulo VI).

La redacción y tipología de los actos criminalizados, así como la sistemática adoptada por la legislación nacional, dejaban notar con claridad la determinante influencia que tuvo sobre sus contenidos y estructura el Convenio sobre la Ciberdelincuencia de Budapest. Lo cual era explicable por ser este instrumento, surgido al interior del Consejo de Europa, el referente internacional más difundido y caracterizado sobre dicha materia. Sin embargo, lo anecdótico en torno a esta fuente legislativa radica en que hasta la fecha el Perú no se ha adherido a dicho documento multilateral como ya lo han hecho otros países latinoamericanos.

Ahora bien, la escasa doctrina nacional que se ha construido sobre la Ley de Delitos Informáticos ha asumido posiciones discrepantes sobre su utilidad y oportunidad. Así por ejemplo, para un sector sólo debieron criminalizarse en ella los delitos informáticos en sentido estricto y no mezclar delitos comunes realiza-

dos a través de sistemas informáticos. En ese sentido NORTHCOTE SANDOVAL sostuvo lo siguiente: "Tal como lo hemos manifestado, la tipificación de estos delitos informáticos nos deja serias preocupaciones sobre su aplicación y posibles efectos en la práctica. Además de las observaciones sobre técnica y sistematización legislativa a que hemos hecho referencia, pues consideramos que estos delitos podrían haberse subsumido en otras figuras generales y, en todo caso, modificar las penas o agravantes de dichos delitos, si la voluntad del legislador era considerar más grave la comisión de un delito por el sólo hecho de haber utilizado tecnologías de la información" (Cristhian Northcote Sandoval). Comentarios a la Ley sobre Delitos Informáticos. Actualidad Empresarial N° 289. Octubre 2013, p. VIII-4).

En cambio, otro sector estimó pertinente el tratamiento conjunto de ambas modalidades de ilícitos, partiendo de la necesidad de sobrecriminalizar un *modus operandi* sofisticado e internacionalizado para la comisión de diferentes delitos convencionales. Al respecto PEÑA CABRERA FREYRE ha destacado que "Es el desvalor de la acción lo que defire la visión de la política criminal plasmada en la Ley de Delitos Informáticos, y no el elemento sistematizador del interés protegido" (Alonso R. Peña Cabrera Freyre). Los Delitos Informáticos: El Uso de Instrumentos Digitales en las Redes Informáticas y en el Ciberespacio. Gaceta Penal 8 Procesal Penal N° 76. Octubre 2015, p. 162).

Por lo demás, cabe precisar que la Ley 30096 y las modificaciones producidas con la Ley 30171 del 10 de marzo de 2014, sólo han tipificado delitos dolosos. La penalidad establecida para los actos criminalizados suele ser conjunta comprendiendo siempre penas privativas de libertas y, según los casos, penas de multa o inhabilitación. Asimismo, en su artículo 11° la Ley de Delitos Informáticos incorpora un catálogo de circunstancias agravantes cualificadas que comprende los siguientes supuestos:

a) Cuando el agente activo integra una organización criminal.
b) Cuando el agente tiene posición especial de acceso a la data o información reservada.
c) Cuando el delito se comete para obtener un fin económico.
d) Cuando el delito compromete fines asistenciales, la defensa, la seguridad y soberanía nacional.

Para todos estos casos la pena privativa de libertad máxima fijada para el delito cometido se incrementa hasta un tercio (Sobre las características dogmáticas de los delitos contenidos en la Ley 30096 véase: Felipe Villavicencio Terreros. Delitos Informáticos. Revista IUS ET VERITAS N° 49. Diciembre 2014, p. 284 y ss.).

A sólo tres años de vigencia la eficacia de la Ley sobre Delitos Informáticos es todavía desconocida en las estadísticas judiciales. Pero, además, quedan varias tareas por realizar para la debida realización de sus objetivos, sobre todo el constituir unidades especializadas en el Ministerio Público y el Poder Judicial, así como de dotar a estas instituciones y a la Policía Nacional de mejores recursos para el funcionamiento eficiente de laboratorios de informática forense. En la actual coyuntura de resurgimiento de prácticas de corrupción organizadas que comprometen en la región a autoridades de alta jerarquía tal requerimiento se torna indispensable.

Rusia

Dra. Svetlana Paramonova.
Brussels, Belgium

I. Definition and Classification

In the hyperconnected world of tomorrow, it will become hard to imagine a "computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity[1].

Until now, there is no a universal definition of `cybercrime. "Definitions' of cybercrime mostly depend upon the purpose of using the term.

In principle, all types of crime that belong to the so-called construct "cybercrime' are divided into two groups: **`core` cybercrime** and **computer-related offenses**[2]. A limited number of acts against the confidentiality, integrity and availability of computer data (information) or systems represent the core of cybercrime, such as illegal access to a computer system, illegal access, and interception or acquisition of computer data. Computer-related offenses are any criminal acts that involve electronic evidence. They can be committed for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts, e.g., computer-related fraud or forgery, computer-related identity offenses, computer-related copyright and trademark offenses, and distribution or possession of child pornography.

II. Criminalization

The UN Comprehensive Study on Cybercrime[3] shows that while worldwide high-level consensus exists regarding broad areas of criminalization, detai-

led analysis of the provisions in source legislation reveals divergent national approaches[4].

The analysis of the Russian legislation regarding criminalization of cybercrime reveals that it follows certain tendencies that comply with the conclusions of the UN study on cybercrime; here, some characteristics of legal regulation shall be emphasized.

The **Criminal Code of the Russian Federation** (CC RF)[5] contains special provisions that are related to the so-called `core` cybercrime. Chapter 28 of the Criminal Code "Crimes in the Field of Computer Information" provides for these offenses. All other crimes that involve any kind of electronic evidence are considered to be "computer-related offenses". For example, computer-related fraud that is addressed as `fraud in the field of computer information `, art. 159.6 CC RF, is classified as an economic crime that involves electronic evidence[6].

According to the Russian criminal law, the ***"core" cybercrime*** include the following ones:

- *unlawful access to computer information* (art. 272 CC RF). It is an unauthorized access to the computer-protected computer data/information that is criminally punishable, if it entails the destruction, blocking, modification or copying of computer information;
- *creation, use and distribution of malicious computer programs* (art. 273 CC RF). It is criminalized, if creation, distribution or use of computer programs or other computer data is knowingly intended for the unauthorized destruction, blocking, modification, copying of computer data or for neutralization of protection facilities of computer data;
- *violation of the rules for the operation of storage facilities, processing or transmission of computer information and of telecommunications networks* (art. 274 CC RF). This violation of the rules is criminally punishable, if it resulted in the destruction, blocking, modification or copying of computer data that caused major damage[7].

In contrast to art. 273 CC RF that belongs to a "**conduct crime**" **(formal crimes)**, both art. 272 CC RF and art. 274 CC RF are "**result crimes**" **(material crimes)**. In the case of "conduct crimes", negligence can be applied merely to socially dangerous behavior, the occurrence of the harmful consequences (which is an obligatory condition for "**result crimes**") is irrelevant for criminal liability. However, whether formal crimes in general can be committed with negligence is a controversial issue in the doctrine[8]. According to the majority opinion, they cannot be committed with negligence by reason that `conduct crimes` as such implicate the intentional commission (e.g., creation of malicious computer programs such as computer virus, art. 273 CC RF)[9]. Negligence as well as intent refers to the present and future circumstances of the situation, which the offender realizes (or should and could realize) at the time of committing a crime[10].

Other cybercrime, according to the Russian criminal law, such as breach of privacy or data protection measures, computer-related fraud or forgery, computer-related identity offenses, computer-related copyright and trademark offenses, distribution or possession of child pornography, computer-related acts involving racism or xenophobia, computer-related acts in support of terrorism offenses, are classified as ***"computer-related offenses"***.

For instance, art. 159.6 CC RF is a cyber-specific crime for computer-related fraud and identity theft committed by means of computer data and telecommunications networks. Cyber-specific provisions explicitly criminalize illegal dissemination through telecommunications networks of pornographic materials (art. 242 pa. 3 CC RF) and child pornography (art. 242 pa. 1 CC RF). A terrorism support offense such as public appeals for the implementation of terrorist activities or the public justification of terrorism, art. 205.2 pa. 2 CC RF, is considered to be a more serious crime, if committed with the use of mass media or electronic or telecommunications networks, including the Internet.

III. Limits of the Application of Domestic Law in Relation to Transnational Cybercrime[11]

Criminal law —in contrast to the possibilities of the Internet— is mainly restrained to its domestic application (primarily to the state territory). However, under the terms of the international law, the **extraterritorial application** of domestic law is not considered a priori as inadmissible[12]. According to **the jurisprudence and the doctrine, n**ational legislation may refer to the extraterritorial application, if there is a clear domestic nexus[13].

An extraterritorial effect is of a particularly great relevance with regard to cybercrime, since these offenses can easily have an impact on several states, even if they have been committed outside of their territories.

– ***The national character of the conflict law in criminal cases***

In Russia, criminal jurisdiction is regulated by the provisions related to "*operation of criminal law in time and space*" (art. 9-13 CC RF). For comparison, in German legal system, the terms "Strafanwendungsrecht" or "internationales Strafrecht" are traditionally used for

the rules on the application of domestic criminal law. In the U.S., relevant jurisdictional rules are comprised by the term "criminal jurisdiction"[14]. In all three mentioned legislative systems, these provisions determine the same matter: **scope of the application of national criminal law**.

Jurisdictional rules regarding criminal matters define the scope of application of national criminal law unilaterally. Possible conflicts of law with other national legal orders are not taken into consideration. Consequently, the criminal law provisions on jurisdiction do not represent conflict of laws in the proper sense. Thus, Russian as well as German criminal codes contain in terms of conflict-of-law rules only such provisions that determine the scope of application of their *own* domestic criminal law. On the contrary, for instance, private international law decides in a concrete case on the most appropriate jurisdiction based on certain links, e.g., nationality or registration of the provider[15].

– Transnational crime and national responsibility

Due to the cross-border nature of the cyberspace, transnational cybercrime, especially offenses related to dissemination of content, terrorism support offenses, computer-related fraud, forgery and identity offenses, cannot be longer effectively prevented only by domestic means. "The classic criminal law based on the territorial sovereignty" will always reach its national borders[16]. Mechanisms of the international criminal justice are applicable only to a limited number of offenses and individuals. Under art. 5 of the Rome Statute[17] the International Criminal Court (ICC) has jurisdiction over core crimes, such as genocide. International criminal law in general refers to the protection of fundamental legal interests and values of the global community. However, the establishment of international military tribunals, ad hoc tribunals as well as existence of the ICC represents an exception and does not change the basic principle of the national nature of the criminal responsibility.

Convention of the Council of Europe on Cybercrime[18] is the only multilateral agreement, which contains regulations that are devoted to jurisdiction issues in cyberspace (art. 22 Convention). It is also open to non-members of the Council of Europe. However, the Convention does not solve the problem of criminal jurisdiction even for the parties to the agreement[19], since "this Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law" (art. 22 pa. 1 Convention). Within the global context, at the U.N. level, there is no any kind of binding legal agreement on cybercrime (convention, protocols, etc.)[20].

– International Cybercrime (Jurisdiction) Court

Today, more and more of the legally protected interests are affected by the cybercrime. The number of the serious offenses committed online increases, becoming more common, and the methods of committing crimes constantly evolve. The potential of cybercrime can easily reach the severity of the "core crimes" of the "Rome Statute", e.g., instructions to the construction of nuclear weapons that could be available online. Moreover, nowadays, critical infrastructures such as water distribution systems, electricity grids, sewage as well as databases of various kinds, such as medical databases, are controlled by the telecommunication technologies. Cyberattacks against such infrastructures have the potential to cause harm to the communities in different states in a new and serious manner.

Due to the negative developments in virtual space — that have very tangible effect in a real world— the establishment of a supranational authority on jurisdiction can become inevitable. Therefore, it is possible that the establishment of an International Institution for Cybercrime (**International Cybercrime Court**) will be required in the future. Primarily, the Court shall deal with resolving jurisdictional conflicts. Its competence could be restricted to only cybercrime that have reached a certain damage threshold.

Bibliography

Akehurst M. 1972. Jurisdiction in International Law, 1972-3 46. British Yearbook of International Law.

Ambos K., Steiner Ch. 2001. Vom Sinn des Strafens auf innerstaatlicher und supranationaler Ebene. JuS. Vol. 1, p. 9 ff.

Ambos K. 2011. Internationales Strafrecht. 3. Ed., Munich.

Babarykin P. V., Kitaev K.K. 2001. K voprosu o jurisdikzii pri rassmotrenii komputernih prestuplenij. Saint Petersburg: Institut avtomatizazii i informatizazii, p. 41 ff.

Babkin S. A. 2006. Intellektualnaya sobstvennost´ v Internete. UrInfor, Moscow, 2006.

Bachin S. 2007. Mezhdunarodnaya sostavlyauschaya pravovoi sistemi Rossii. Правоведение (Pravovedenie), Vol. 6, p. 126.

Barton D.-M. 1999. Multimedia-Strafrecht. Ein Handbuch für die Praxis. Neuwied.

Bremer K. 2001. Strafbare Internet-Inhalte in internationaler Hinsicht. Ist der Nationalstaat wirklich überholt? Frankfurt am Main.

Brenner W., Koops B.-J. 2004. Approaches to Cybercrime Jurisdiction. 4 J. High Tech. L. 2004, p. 1 ff.

Cornils K. 1999. Der Begehungsort von Aüßerungsdelikten im Internet. Vol. 8, JZ. p. 394 ff.

Dorfmann M. 2006. Zeitschrift Pravo i politika. N 11. Available at: http://www.nbpublish.com/lpmag/single_mag.php?id=&month=11&year=2006.

Gavrilov V. 2005. Ponyatie i vzaimodejstvie mezhdunarodnoj i nazionalnoj pravovich system. Vladivostok, p. 11.

Gercke M. 2009. Understanding Cybercrime – A Guide for Developing Countries. www.itu.int/ITU-D/cyb/…/itu-understanding-cybercrime-guide.pdf.

Goode M. 1997. The Tortured Tale of Criminal Jurisdiction. Melbourne University Law Review.

Grinuyk M. 2004. Internet. Ego jurisdikzija (Internet. Seine Jurisdiktion). Pravo i Internet, www.allpravo.ru.

Guinchard A. 2007 Criminal Law in the 21-st century: the demise of territoriality. University Essex. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=12900.

Ivanenko V. 2010. Mezhdunarodnie dogovori i konstituziya v pravovoj sisteme Rossii. Правоведение (Pravovedenie), Vol. 3, pp. 135-161.

Jakuschev M.A. 1997. Internet i pravo (Das Internet und das Recht). Zakonodatelstvo, Vol. 1.

Jescheck H. H., Gribbohm G., Schünemann B., Schroeder F.Ch., Jähnke, B., Hillenkamp, T., Lilie H., AlbrechtD., Roxin C. 1997. Leipziger Kommertar zum StGB. 11. Ed., Berlin, New York.

Jescheck H.-H., Weigend Th. 1996. Strafrecht Allgemeiner Teil. 5. Ed., Berlin.

Kälin W., Epiney A. 2003. Völkerrecht. Einführung. Verlag AG. Bern.

Kaufmann C. 2008. Das Verhältnis von Völkerrecht und Landesrecht. Available at: http://www.unserrecht.ch/fileadmin/user_upload/files/Christine_Kaufmann__Voelkerrecht_und_Landesrecht.pdf.

Kegel G., Schurig K. 2004. Internationales Privatrecht. 9. Ed., Munich.

Kohl U. 2007. Jurisdiction and the Internet. Cambridge University Press.

Kropachev N. M. 2010. Rossijskoe Ugolovnoe Pravo. Obschaja Chast. Saint Petersburg.

Kudlich H. 2004. Herkunftslandprinzip und internationales Strafrecht. Vol. 8, HRRS, p. 278 ff.

Kudrjavzev V. N. 1999. Mezhdunarodnoe ugolovnoe pravo (Internationales Strafrecht). 2. Ed., Nauka. Moscow.

Ladeur K.-H. 1997. Zur Kooperation von staatlicher Regulierung und Selbstregulierung des Internets. ZUM, p. 359 ff.

Lehle Th. 1999. Der Erfolgsbegriff und die deutsche Strafrechtszuständigkeit im Internet. 1. Ed. Konstanz.

Loskutov I. 2008. Sravnitelnij analis mezhdunarodnih norm zakonodatelnogo regulirovanija Interneta v razlichnih stranah, Available at: http://www.medialaw.kz.

Malanczuk P. 2010. Akehurst's modern introduction to international law. 8. Ed., London.

Mankowski P., Bock S. 2008. Die internationale Zuständigkeit der deutschen Strafgerichte als eigene Kategorie des Internationalen Strafverfahrensrechts. JZ, p. 505 ff.

Mayer F. C. 1996. Recht und Cyberspace. NJW, p. 1782 ff.

Naumov A. V. 2007. Rossijskoe Ugolovnoe Pravo.

Oehler D. 1973. Internationales Strafrecht. Cologne, Berlin, Bonn, Munich.

Paramonova, S. Internationales Strafrecht im Cyberspace: Rechtslage in Deutschland, Russland und den USA (Criminal Jurisdiction in Cyberspace: Legal Analysis of German, Russian, and US-American Law). Berlin, Springer-Verlag, 314 p., 2013: http://www.springer.com/gp/book/9783658043988.

Paramonova, S. Challenges for Criminal Law and International Criminal Law in Cyberspace. In: Justice Report. Canadian Criminal Justice Association, 2014, Issue/Volume 29, nº 4, pp. 26-29.

Paramonova S. 2011. Concept and systematization of the criminal offense in Russia. In: Sieber, U. / Forster, S. / Jarvers, K. (ed.): National Criminal Law in a Comparative Legal Context. Volume 3.1: Defining criminal conduct. Berlin, Duncker & Humblot, p. 86-97 (cit.: Paramonova, Concept and systematization of the criminal offense in Russia. In: National Criminal Law in a Comparative Legal Context).

Paramonova S. 2011. Extraterritorial jurisdiction in Russia. In: Sieber, U. / Forster, S. / Jarvers, K. (ed.): National Criminal Law in a Comparative Legal Context. Volume 2.1: General limitations on the application of criminal law. Berlin, Duncker & Humblot, p. 297-315 (cit.: Paramonova, Extraterritorial jurisdiction in Russia. In: National Criminal Law in a Comparative Legal Context).

Paramonova S. 2010. The Principle of Universality and Extradition in Russia. Revista Penal, Vol. 26, pp. 220-223.

Paramonova S. 2009. Ugolovnaya jurisdikziya v Internet-prostranstve: terroritorial´nij prinzip v rossijskom i nemezkom zakonodatelstve (Criminal Jurisdiction in Cyberspace: Principle of Territoriality). Zhurnal zarubezhnogo zakonodatelstva i sravnitelnogo pravovedeniya, Vol. 4, p. 77-84.

Primig Th. J. Internationales Strafrecht und das Internet. Available at: http://www.rechtsprobleme.at/doks/primig-1-internationales_strafrecht.pdf.

Rath J. 2006. Prüfungsschema. Auslandsbezug. Tatortbestimmung. JA. p. 453 ff.

Romaschkin P. S. 1946. K voprosu o ponjatii i istochnikah mezhdunarodnogo ugolovnogo prava.

Schönke A., Schröder H., Eser A. Strafgesetzbuch. 2010. Kommentar. 28. Ed., Munich.

Sieber U. Grenzen des Strafrechts. 2007. Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht. Vol. 119, ZStW, p. 1 ff.

Suter M. 2007. A Generic National Framework for Critical Information Infrastructure Protection. Available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

Uschakov N. A. 2000. Mezhdunarodnoe pravo. Moscow.

Weber G. 2008. Völkerstrafrecht. 2. Ed.

Werle J. 2001. Grundfälle zum Strafanwendungsrecht. Vol. 1, JuS, p. 35 ff.

Wigert, Isabelle. 2006. Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security. IIB-1.

Wilshusen G. *2007. Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy. GAO Document GAO-08-212T. Available at: http://www.gao.gov/new.items/d08212t.pdf.*

List of abbreviations

alter.	alternative
art.	article, articles
p.	page/pages
pa.	part
RF	Rossijskaya Federaciya (Russian Federation)
CC RF	Ugolovnij Kodeks Rossijskoj Federazii (Criminal Code of the Russian Federation)
StGB	Strafgesetzbuch (German Criminal Code)
Vol.	volume

Notas

1 UN Comprehensive Study on Cybercrime 2013.

2 UN Comprehensive Study on Cybercrime 2013; *Paramonova*, Internationales Strafrecht im Cyberspace: Rechtslage in Deutschland, Russland und den USA (Criminal Jurisdiction in Cyberspace: Legal Analysis of German, Russian, and US-American Law). Berlin, Springer-Verlag, 2013: http://www.springer.com/gp/book/9783658043988; *Gercke,* Understanding Cybercrime. www.itu.int/ITU-D/cyb/…/itu-understanding-cybercrime-guide.pdf.

3 Information on cybercrime criminal laws was gathered through the study questionnaire, as well as by primary source analysis of available legislation collected by the Secretariat. Primary source legislation was analyzed for 97 Member States, including 56 that responded to the questionnaire, with regional distribution as follows: Africa (15), Americas (22), Asia (24), Europe (30), and Oceania (6).

4 The study questionnaire referred to 14 acts commonly included in notions of cybercrime: Illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal data interference or system interference; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offenses; computer-related copyright and trademark offenses; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution or possession of child pornography; computer-related solicitation or "grooming" of children; and computer-related acts in support of terrorism offenses.

5 *Criminal Code of the Russian Federation*, 17.06.1996, N 63-ФЗ: http://www.consultant.ru. Further CC RF.

6 *Federal Law* 29.11.2012 N 207-ФЗ.

7 *Paramonova*, Criminal Jurisdiction in Cyberspace Springer, 2013: http://www.springer.com/gp/book/9783658043988.

8 *Kropachev*, Ugolovnoe pravo Rossii, p. 482.

9 *Lebedev*, Kommentarii k Ugolovnomu Kodeksu RF, p. 57; *Naumov*, Rossiiskoe ugolovnoe pravo, p. 381.

10 *Paramonova*, Subjective aspects of the offense in Russia. In: Sieber, U. / Forster, S. / Jarvers, K. (ed(s).): National Criminal Law in a Comparative Legal Context. Volume 3.1: Defining criminal conduct. Berlin, Duncker & Humblot, 2011, pp. 442-443.

11 *Paramonova*, Boundlessness of Cyberspace vs. Limited Application of the National Criminal Law. International Cybercrime Court. In: Journal: Grigol Robakidze University Academic Digest, 2013, N 2. p. 38-51.

12 See: *The report on Extraterritorial Criminal Jurisdiction.* Council of Europe, European Committee on Crime Problems, 1992, p. 447 ff.; Lotus case, C.P.J.I. Ser. A. nº. 10, 1927.

13 Lotus case, C.P.J.I. Ser. A. nº. 10, 1927; BGHSt 46, 212.

14 *CFAA* 1984, 18 U.S.C. § 1030 ff.

15 *Paramonova*, Criminal Jurisdiction in Cyberspace. Springer, 2013.

16 The European Arrest Warrant allows a certain extraterritoriality of the criminal justice: *EuHbG*, 2006.

17 http://www.un.org/law.

18 Convention on Cybercrime, 23.11.2001: http:// http://conventions.coe.int/Treaty.

19 Signatures and ratifications of the Convention on Cybercrime, 23.11.2001: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG: USA and Germany ratified the Convention; Russia did not ratify and in 2008 withdrew its signature.

20 "I´m not Willing to Accept Deadlock", *Stein Schjolberg*. 20 March 2012 (posted by Thomas Lynch): http://www.ewi.info/i-am-not-willing-accept-deadlock.

Ucrania

Volodymyr Hulkevych

Doctor en Derecho, Fiscalia de la provincia de Ivano-Frankivsk

El concepto de los delitos cibernéticos es relativamente nuevo, en el derecho internacional y en la legislación de los estados individuales. De acuerdo con el Convenio sobre la Ciberdelincuencia, firmado el 23 de noviembre de 2001 por los países-miembros del Consejo de Europa y por otros países, y con el Protocolo Adicional al presente Convenio firmado el 28 de enero de 2003, se refieren a los delitos cibernéticos, falsificaciones, fraudes, pornografía infantil, violaciones de los derechos de autor y de los derechos conexos, violaciones de la seguridad de las redes de computadora, propagación de materiales racistas y xenófobos, amenazas y ataques, que se cometen usando computadoras y redes internacionales de Internet.

En la legislación nacional, el concepto del delito cibernético todavía no se ha definido, lo que genera ciertas discusiones a nivel teórico. Sin embargo, algunas infracciones de las leyes ya se han reconocido como crímenes.

La responsabilidad penal por los delitos cibernéticos en Ucrania fue introducida por primera vez mediante la aprobación el 05 de abril de 2001 del nuevo Código Penal de Ucrania, en que apareció una sección XVI "Delitos en el ámbito del uso de máquinas de información electrónicas (de computadoras), de sistemas y redes de computadoras", la cual consta de 3 artículos. Para hoy día, esta sección se llama "Delitos en el ámbito del uso de máquinas de información electrónicas (de computadoras), sistemas y redes de computadoras y redes de telecomunicaciones", y consta de 6 artículos.

En la doctrina nacional del derecho penal sigue siendo la idea dominante sobre el reconocimiento como un bien jurídico del delito de las relaciones públicas. Conformemente, los científicos nacionales reconocen como bien jurídico de los delitos, determinados por la sección XVI del Código Penal "las relaciones de información en el campo de aplicación de las máquinas de computación", "las relaciones sociales en el área de aplicación de los sistemas de computadoras" o "un conjunto de relaciones sociales que aparecen con relación al procesamiento (la recolección, la introducción, la grabación, la conversión, la lectura, el almacenamiento, la destrucción, el registro), a la protección de la información de computadora y de la operación de los medios que las aseguran (de los sistemas de computadoras y de las redes de telecomunicaciones)".

En la parte 1 del art. 361 del Código Penal se ha establecido la responsabilidad penal por la interferencia no autorizada en el funcionamiento de las máquinas de computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes de ordenadores o de las redes de telecomunicaciones, lo que condujo a la filtración, a la pérdida, a la falsificación, al bloqueo de la información, a la distorsión del procesamiento de la información o a la violación del orden establecido de enrutamiento de la misma. Las referidas acciones son punibles con una multa de seiscientos a mil ingresos mínimos libres de impuestos de los ciudadanos, o con la restricción de la libertad a un término de dos a cinco años, o con la privación de la libertad a un término de hasta tres años, con la inhabilitación para ocupar determinados cargos o realizar ciertas actividades durante un máximo de dos años, o sin tal.

Como objeto material de este delito se reconoce la información de ordenador o la información que se transmite por las redes de telecomunicaciones.

El sujeto activo del delito es común, es decir una persona física imputable que ha llegado a los 16 años de edad. El tipo subjetivo del delito es caracterizado por intención directa o indirecta.

En la parte 1 del art. 361[1] del Código Penal se ha establecido la responsabilidad penal por la creación con el propósito del uso, distribución o comercialización, así como de la distribución o comercialización de software o hardware dañinos diseñados para la interferencia no sancionada en el funcionamiento de las máquinas de computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes informáticas o de las redes de telecomunicaciones. Estas acciones son punibles con una multa de quinientos a mil ingresos mínimos libres de impuestos de los ciudadanos, o con trabajos correccionales a un término de hasta dos años, o con la privación de la libertad para el mismo término.

Como objeto material del delito son software o hardware dañinos diseñados para la interferencia no sancionada en el funcionamiento de las máquinas de

computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes de ordenadores o de las redes de telecomunicaciones. Es fácil comprender que una parte de las acciones previstas en la parte 1 del art. 361[1] del Código Penal, es la preparación para cometer un delito especificado en el artículo anterior del Código.

El sujeto activo del delito es común. El tipo subjetivo del delito se caracteriza por una intención directa de la creación de software o hardware maliciosos destinados para la interferencia no sancionada en el funcionamiento de las máquinas de computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes de ordenadores o de las redes de telecomunicaciones, y también con el propósito de uso, distribución o comercialización de los mismos.

En la parte 1 del art. 361[2] del Código Penal está prevista la responsabilidad penal por la comercialización o distribución no sancionadas de la información con acceso restringido, la cual se almacena en las máquinas de computación electrónicas (en las computadoras), en los sistemas automatizados, en las redes de computadoras o en los portadores de dicha información creada y protegida de acuerdo con la legislación aplicable. Estas acciones son punibles con una multa de quinientos a mil ingresos mínimos libres de impuestos de los ciudadanos, o con la privación de la libertad a un término de hasta dos años.

Como objeto material del delito se reconoce la información con acceso restringido que se almacena en las máquinas de computación electrónicas (en las computadoras), en los sistemas automatizados, en las redes de computadoras o en los portadores de dicha información creada y protegida de acuerdo con la legislación aplicable.

El sujeto activo de un delito es común. El tipo subjetivo del delito se caracteriza por una intención directa.

De acuerdo con la parte 1 del art. 362 del Código Penal, la alteración, la eliminación o el bloqueo de la información no autorizados, la cual se procesa en las máquinas de computación electrónicas (en las computadoras), en los sistemas automatizados, en las redes de computadoras o se almacena en los portadores de dicha información, cometidos por una persona que tenga derecho de acceso a la misma, serán castigados con una multa de seiscientos a mil ingresos mínimos libres de impuestos de los ciudadanos, o con trabajos correccionales a un término de hasta dos años.

Como objeto material de este delito es una información de computadora.

Conforme a la parte 2 del art. 362 del Código Penal, las intercepciones o copias no autorizadas de la información que se procesa en las máquinas de computación electrónicas (en las computadoras), en los sistemas automatizados, en las redes de computadoras o se almacena en los portadores de dicha información, si esto llevó a su filtración, cometidas por una persona que tiene el derecho de acceso a tal información, se castigará con la privación de la libertad a un término de hasta tres años con la inhabilitación para ocupar ciertas posiciones u ocuparse de ciertas actividades para el mismo período.

Como objeto material del delito es la informática de computadora, el acceso a la cual es limitado, dado que la única consecuencia de este delito es la filtración de la información, con el que es imposible reconocer la filtración de la información que está a disposición del público.

El sujeto activo del delito mencionado es especial, es decir una persona que tenía el acceso a la información de la computadora. El tipo subjetivo del delito si fue cometido en la forma de intercepción de la información, se caracteriza por la intención directa. Otras acciones previstas en este artículo, pueden ser cometidas tanto intencionalmente, como imprudentemente.

De conformidad con el art. 363 del Código Penal, como delito se ha reconocido la violación de las reglas de operación de las máquinas de computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes de ordenadores o de las redes de telecomunicaciones o del orden o de las reglas de protección de la información que se procesa en los mismos, si esto ha causado un daño significativo, cometidos por una persona responsable por la operación de las mismas. Los referidos actos son punibles con una multa de quinientos a mil ingresos mínimos libres de impuestos de los ciudadanos, o con la restricción de la libertad a un término de hasta tres años, con inhabilitación para ocupar determinados cargos u ocuparse de ciertas actividades durante el mismo período.

Como objeto material del delito, se reconoce una información de la computadora o una información transmitida por las redes de telecomunicaciones.

El sujeto activo del delito es especial. Como sujeto activo del mismo puede ser una persona responsable por la operación de las máquinas de computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes de ordenadores o de las redes de telecomunicaciones. El tipo subjetivo del delito es caracterizado por la actitud intencional o negligente del sujeto a su acción o inacción ya las consecuencias de las mismas -por la actitud exclusivamente negligente.

En la parte 1 del art. 363[1] del Código Penal, se reconoce como delito la distribución de masas premeditada de los mensajes transmitidas por las redes de telecomunicaciones, la cual se ha efectuado sin el consentimiento previo de los destinatarios, lo que ha llevado a la perturbación o interrupción del funcionamiento de las máquinas de computación electrónicas (de las computadoras), de los sistemas automatizados, de las redes de ordenadores o de las redes de telecomunicaciones. Estas acciones son punibles con una multa de quinientos a mil ingresos mínimos libres de impuestos de los ciudadanos, o con la restricción de la libertad a un término de hasta tres años.

Como objeto material del delito es una información de la computadora o la información transmitida por las redes de telecomunicaciones.

El sujeto activo del delito es común. El tipo subjetivo es caracterizado por la culpa en la forma de la intención directa o indirecta.

En la parte 2 del art. 361, parte 2 del art. 361[1], parte 2 del art. 361[2], parte del 363[1] y la parte 3 del art. 362 del Código Penal se establece una mayor responsabilidad penal por actos previstos por descritas anteriormente las partes 1 del art. 361, 361[1], 361[2], 363[1] y por las partes 1, 2 del art. 362 del Código Penal, cometidos repetidamente o por un acuerdo previo por un grupo de personas, o si los mismos causaron un daño considerable. Conforme a la nota para el art. 361 del Código Penal, como daños considerables en los art. 361-363[1] del Código Penal, si estos consisten en perjuicios materiales, se consideran tales daños que superen los ingresos mínimos libres de impuestos de los ciudadanos a cien veces y a más.

El tipo objetivo de los delitos previstos por el art. 361, 361[1], 361[2], 362 y 363[1] del Código Penal se caracteriza por acciones activas. El delito definido en el art. 363 del Código Penal puede ser cometido tanto en la forma de acciones, como por omisión imprudente.

Un número significativo de los términos contenidos en los artículos mencionados del Código Penal, se definen por otras leyes y reglamentos, por tales, como, por ejemplo, las Leyes de Ucrania "Sobre las telecomunicaciones", "Sobre la protección de la información en los sistemas de telecomunicaciones" y por otras. Por lo tanto, la correcta aplicación de los artículos de la Sección XVI del Código Penal requiere la correcta interpretación de las normas de las leyes especificadas.

Además, el Código Penal contiene un artículo más, en que están previstas sanciones penales por el delito cometido, el que puede ser llamado como un delito cibernético en la comprensión de la Convención sobre la delincuencia cibernética.

En particular, de acuerdo con la parte 3 del art. 190 del Código Penal se castiga con la privación de la libertad a un término de tres a ocho años un fraude cometido mediante transacciones ilegales utilizando máquinas de computación electrónicas. Este delito consiste en el uso engañoso o a través del abuso de confianza, de las capacidades y medios de tales máquinas, el cual está relacionado con la introducción deliberada (con la colocación) en el sistema electrónico de las mismas de los datos relevantes que son identificados por el referido sistema como tales que si hubieran sido introducidos por el propietario (por la persona autorizada), y a aquel defraudador se le concede la oportunidad de obtener una cierta cantidad de dinero ajeno.

Esto quiere decir que el Código Penal en vigor contiene una serie de delitos, los cuales pueden ser llamados como los delitos cibernéticos en la comprensión de la Convención sobre la delincuencia cibernética. Por lo tanto, sería aconsejable resolver el problema de la criminalización relacionada con falsificaciones, pornografía infantil, violaciones de los derechos de autor y derechos conexos, difusión de materiales racistas y xenófobos, amenazas y ataques, que se cometen con ayuda de los ordenadores y la red global de Internet.

Bibliografía

Kryminalnyi kodeks Ukrainy. Naukovo-praktychnyi komentar: za zah. red. V.J. Taciia, V.P. Pszonky, V.I. Borysowa, V.I. Tiutiuhina. 5-te vyd., dopov. T. 2: Osoblyva chastyna (en ucraniano) // El Código Penal de Ucrania. Comentario. La edición quinta modificada y completada. La redacción a cargo de V.I. Tacii, V.P. Pszonka, V.I. Borysov, V.I. Tiutiuhin, Kharkiv, 2013.

Naukovo-praktychnyi komentar Kryminalnoho kodeksu Ukrainy. Za zah. red. O.M. Dzhuzhi, A.V. Savchenka, V.V. Cherneia (en ucraniano) // Comentario cientifico-pratico al Código Penal de Ucrania. La redacción a cargo de O.M. Dzhuzha, A.V. Savchenko, V.V. Chernei, Kyiv, 2015.

Karchevskyi M.V. Kryminalna vidpovidalnist za nezakonne vtruchannia v robotu elektronno-obchysluvalnyh mashyn (kompiuteriv), system ta kompiuternyh merezh (analiz skladu zlochynu) (en ucraniano) // La responsabilidad penal por la interferencia ilegal con el funcionamiento de los ordenadores, sistemas y redes (análisis del delito), Harkiv, 2003.

Orlov S.O. Kryminalno-pravova ohorona informacii v kompiuternyh systemah ta telekomunikaciinyh merezhah (en ucraniano) // La protección penal de la iformación en los sistemas informáticos y redes de telecomunicaciones, Harkiv, 2004.

Rosenfeld N.A. Kryminalno-pravova harakterystyka nezakonnoho vtruchannia v robotu elektronno-obchysluvalnyh mashyn (kompiuteriv), system ta kompiuternyh merezh (en ucraniano) // La característica penal de la interferencia ilegal en la operación de los ordenadores, sistemas informáticos y las redes de ordenadores, Kyiv, 2003

Uruguay

Pamela Cruz/Sofía Lascano[1]

1. Este informe refiere a la categoría "delitos informáticos" en el ordenamiento jurídico penal de Uruguay. Esta es una nueva categoría derivada del avance tecnológico, mediante la cual se pueden llegar a cometer ilícitos penales relacionados con la transmisión de datos y con la confianza o certeza en las comunicaciones, que son de tal gravedad que ameritan tipificarse como delitos. Para que ellas sean legítimas, tales tipificaciones deberían ser consecuencia de la protección de bienes jurídicos de interés relevante para que dichas conductas merezcan la amenaza de una pena. Al momento de la tipificación habrá que tener en cuenta la opinión de la doctrina para decidir si los nuevos tipos penales se adaptan a la nueva realidad que ya no puede ser abarcada por los tipos penales existentes[2].

2. La Organización para la Cooperación y Desarrollo Económico (OCDE) define al delito informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos". En relación a esto, surgen las siguientes preguntas: ¿Qué elementos problemáticos tiene esta definición?; ¿Qué diferenciaría entonces a un delito informático de un delito tradicional?; ¿hacer esta clasificación sería útil o tendría sentido?

En el presente se intentará dar respuestas (no definitivas) a estas y otras cuestiones vinculadas, sin tener la intención de dar tratamiento a conceptos técnicos al respecto, y sin perjuicio de tratarse de un debate actual y de alcance internacional, el cual intentaremos acotar puntualmente al Uruguay.

3. "El procesado automático de datos y/o transmisiones de datos" del que habla la definición anteriormente citada, no es más que una especie dentro de la categoría que llamamos "medios informáticos o electrónicos", siendo estos los que, en principio, distinguirían a un delito informático de un delito tradicional. No obstante ello, la controversia se genera respecto a si son estos un medio distinto de comisión del delito tradicional o un elemento típico y caracterizante de un delito nuevo como sería o debiera ser el delito informático. La mutabilidad, dinámica, transnacionalidad y versatilidad como características de los medios informáticos, cuestionan la utilidad del derecho penal como instrumento de regulación y sanción.

4. En el caso uruguayo, se habla concretamente de falta de regulación en el ámbito de los delitos informáticos, ya que no existe normativa penal específica[3]. Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El art. 7 de la Ley 17.815, afirma que "constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales"., permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación[4].

5. Ahora bien, si entendemos que los medios informáticos son estricta y exclusivamente medios, podemos decir que un tipo penal tradicional como por ejemplo, la figura de la Estafa (Artículo 347 del Código Penal Uruguayo), sería aplicable sin inconvenientes a la llamada "Estafa Informática". De hecho así se observa aplicada por los jueces uruguayos, tal como se dispuso en la Sentencia nº. 230 del 11 de noviembre del 2005 emanada de la Suprema Corte de Justicia del Uruguay, la cual desestima el recurso de casación interpuesto para la Sentencia nº. 397 dictada por el Tribunal de Apelaciones en lo Penal de Segundo turno. El tribunal de alzada desestima el recurso interpuesto por la defensa confirmando la condena de un delito continuado de estafa. "(…) los enjuiciados, mediante la utilización de tarjetas no provenientes del Ente oficial, obtuvieron la "llave" para integrar al sistema de comunicación telefónica por cable, logrando de tal modo comunicarse con abonados residentes en diversos puntos del Planeta, privando a A.N.T.E.L. de la percepción de prestaciones de contenido económico, con motivo de la realización del servicio y que el organismo estatal estimó en $ 370.000. (…) Ello determinó que el

Tribunal subsumiera los hechos de autos dentro de la figura de la estafa, regulada por el art. 347 del CP, en tanto mediante el sofisticado mecanismo artificioso se induce en error al sistema electrónico del Ente, con el consiguiente perjuicio para la empresa damnificada y la obtención de un provecho ilícito para los autores de la conducta, teniendo en cuenta que los imputados tuvieron conciencia y voluntad de utilizar tal estratagema para "abrir la llave" de un servicio al cual no tenían derecho a utilizar, ante la falta de la contraprestación realmente debida, o sea, el pago de la cantidad de tarjetas que debieron ser adquiridas, si se hubiere actuado lícitamente"[5].

6. La inquietud surge cuando observamos que existen conductas que, de relacionarse con medios informáticos, parecen no estar contempladas en los delitos tradicionales, por ejemplo, hablar de modalidades de tráfico de base de datos, modificaciones de programas y sabotaje informático (con sus sub-modalidades), entre otros. Aquí es donde se presenta un nuevo escenario, que, criminológicamente hablando, se ha dado en llamar "cibercriminalidad". Al parecer, de este nuevo escenario el Uruguay estaría, en principio, desprotegido.

7. La cibercriminalidad entonces, como rama de la criminología, pretende visibilizar "cómo influye el ciberespacio en la configuración de la delincuencia, si es un facilitador de determinadas tipologías delictivas y que características aporta en la delincuencia"[6]. Esta nueva delincuencia como realidad social y concreta, requiere para ser entendida de estudios pormenorizados e interdisciplinarios a efectos de determinar, entre otras cosas y en lo que a nosotros nos interesa, cuál sería la función o alcance del derecho respecto a ella. Sin llegar a un acuerdo previo sobre este punto, es inútil hablar de por ejemplo, la eficacia o ineficacia de las investigaciones que se realizan en esta área específica.

8. En Uruguay y simplemente para mencionarlo, existe un Departamento de Delitos Informáticos perteneciente a la Dirección General de Lucha contra el Crimen Organizado (DGLCCO) e INTERPOL[7]; quienes colaboran con su labor investigativa. También existe la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), que tiene entre sus cometidos, la función de proponer y asesorar al Poder Ejecutivo en la formulación de políticas en materia de la Sociedad de la Información y del Conocimiento y en el desarrollo informático del Estado; dictar y proponer normas, estándares y procedimientos técnicos en materia informática para el Estado; analizar tendencias tecnológicas en materia informática y su impacto en las políticas, normas, estándares y procedimientos existentes o a proponer (Laboratorio Tecnológico), entre otros relacionados en mayor medida, a la prevención[8].

9. Dichos organismos enfrentan cada día el desafío de entender cómo se producen y quienes son, los responsables detrás de los ataques cibernéticos que afectan al Uruguay, muchos de los cuales tienen repercusión mundial. Estos han demostrado poder colaborar con la implementación de medidas de prevención y protocolos de seguridad por parte de las empresas o sujetos vulnerables, para que estos eviten daños; pero lo que parece desconocerse es que sucede cuando el daño ya se ha producido, es aquí donde surge la incertidumbre acerca del procedimiento a seguir. Obviamente que esto parece ser consecuencia de la falta de tipos penales en el ordenamiento jurídico penal, como ya hemos mencionado.

10. En el derecho comparado, se encuentran diferentes y variadas soluciones como instrumentos al respecto, Estados que tipifican especialmente las conductas vinculadas a la criminalidad informática, Estados que no, y Estados que regulan algunas conductas en forma específica y otras las ingresan dentro de los delitos ya existentes, sean estos contra el honor, el patrimonio, etc. A continuación, algunos datos interesantes[9].

Delito Informático	%
Acceso Ilícito	19%
Interceptación Ilícita	33%
Atentado contra la integridad de los datos	14%
Atentado contra la Integridad del sistema	33%
Abuso de los dispositivos	71%
Falsedad Informática	57%
Fraude o Estafa Informática	48%
Pornografia Infantil	19%

Tabla Nro 3. Estadísticas que indican el porcentaje de los países que aún no tienen sanción penal según cada delito informático analizado.

11. En definitiva y a modo de conclusión, decir que la delincuencia informática quizá como la económica, tan vinculadas entre sí, son un fenómeno en constante cambio, lo cual implica deducir que jurídicamente pareciéramos estar un paso atrás; que regular, implica muchas veces dejar obsoletas figuras que ante la innovación en nuevas modalidades ya no son de utilidad, como por ejemplo sucede con la creación constante de nuevas redes sociales, con la incursión de compañías financieras tecnológicas (Fintech), con el crecimiento acelerado del comercio electrónico, etc;

que si intentamos igual tipificar todas estas conductas y sancionarlas penalmente, entonces el derecho penal dejaría de ser de "ultima ratio".

Notas

1 Integrantes del Observatorio Latinoamericano para la investigación en Política Criminal y en las reformas en el Derecho Penal (OLAP, http://olap.fder.edu.uy/), Universidad de la República, Montevideo, Uruguay.

2 "La tarea del Derecho no es la de quedarse atado a viejas categorías teóricas que nada sirven sino más bien de adaptarse y proveerse de nuevas formas de prevención y protección a la sociedad" … "Es por ello que el Derecho Penal informático debe revisarse así mismo, y encuadrarse en estas situaciones que protejan a las personas y no esconderse en vacíos legales que no nos benefician absolutamente". TIEDEMANN, Klaus (2000) Derecho Penal y Nuevas Formas de Criminalidad, Edit. Idemsa, Lima, p. 267.

3 VIEGA RODRÍGUEZ, María José, Un nuevo desafío jurídico: Los Delitos Informáticos, http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf.

4 TEMPERINI, Marcelo Gabriel Ignacio, Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf.

5 LJU CASO 15377 disponible en: http://www.laleyonline.com.uy

6 GARCÍA LUNA, Julio César y PEÑA LABRIN, Daniel Ernesto, Cibercriminalidad & Postmodernidad: La Cibercriminología como respuesta al escenario contemporáneo, p. 10, como se citó en GONZALES GARCÍA, Abel (2013) p. 4.

7 Por mayor información: https://policia.minterior.gub.uy/index.php/noticias-y-comunicados-de- prensa/1352-delitos-informaticos-crecen-con-los-adelantos-tecnologicos. https://www.minterior.gub.uy/index.php/documentos-y-legislacion/decretos/11-decreto-que-regula-la- direccion-general-de-lucha-contra-el-crimen-organizado-e-interpol. https://www.interpol.int/es/Crime- areas/Cybercrime/Cybercrime.

8 Ver: https://www.agesic.gub.uy/

9 Extraídos de: TEMPERINI, Marcelo Gabriel Ignacio, Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf.

Venezuela

Jesús Enrique Rincón Rincón
Doctor en Derecho. Juez Penal
Profesor de Derecho Penal General y Especial
Profesor de postgrado de Derecho Procesal Penal y Derecho Penal
Miembro de la Academia de Ciencias Jurídicas del Estado Zulia

I. Introducción

El respeto al derecho a la privacidad de las personas y la prohibición de vigilar sus movimientos y conversaciones, sin causa legal justificada, son características que distinguen a un Estado democrático de uno que no lo es. Por ello se dictan leyes que consagran y protegen esos derechos y garantías ciudadanas. En fecha 30 de octubre de 2001, fue publicada en la Gaceta Oficial[1], la Ley Especial Contra Delitos Informáticos, en cuyo artículo 1°, se establece que el objeto de dicha Ley, es "*la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley*".

Diez años antes, el 16 de diciembre de 1991, entró en vigencia la Ley Sobre Protección a la Privacidad de las Comunicaciones[2], la cual es un antecedente muy importante de la actual Ley, pero que, lamentablemente, ni una ley ni la otra, realmente han servido para garantizar la intimidad de las personas, sus datos, su información personal y la confidencialidad de sus comunicaciones con otras personas. Prácticamente se han convertido ambas en letra muerta, sin aplicación práctica ninguna.

Otro antecedente de alguna manera relacionado con este asunto, es el Decreto Ley de Mensajes de Datos y Firmas Electrónicas de 2001 (LMDFE)[3], así como su Reglamento Parcial, de fecha 14 de diciembre de 2004[4], el cual desarrolla el mencionado Decreto-Ley, cuyo objeto principal es el de "*otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas*" (artículo 1).

En la Exposición de Motivos de dicho Decreto-Ley, se indica que a los fines de conceder la seguridad jurídica necesaria para la aplicación de la Ley, así como la adecuada eficacia probatoria a los mensajes de datos y firmas electrónicas, "*se le atribuye a éstos el mismo valor probatorio que la Ley consagra a los instrumentos escritos, los cuales gozan de tarifa legal y producen plena prueba entre las partes y frente a terceros de acuerdo a su naturaleza*". En este mismo sentido, en el artículo 4 se dispone que los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos y a los fines de reforzar ese sistema jurídico de validez de los mensajes electrónicos, la LMDFE exige que para que el documento electrónico tenga plena validez jurídica debe contener otro elemento fundamental, como es la firma electrónica debidamente utilizada con la correspondiente certifica-

ción que garantiza la autoría de dicha firma, tal y como lo exige el artículo 38 *eiusdem*.

Sin embargo, aunque por todos es conocido que uno de los aspectos determinantes para otorgar pleno valor jurídico a los documentos es la firma, pues ésta permite identificar el autor del respectivo documento, este objetivo se cumple con un amplio margen de certeza en los documentos escritos, toda vez que en la escritura se incorporan rasgos psicológicos inconscientes peculiares de cada persona, lo que permite determinar, de manera fehaciente, los casos de falsificación de firmas, adicionalmente al hecho de que muchos se otorgan por ante Notario Público, que da fe del mismo, lo que evita la mayoría de las estafas y los fraudes. Pero, la falta de esos elementos en la firma electrónica, que permita establecer en forma cierta la autoría del documento es, sin duda, la principal debilidad que enfrentan los documentos electrónicos frente a las tradicionales pruebas documentales, y es por ello que su uso no se ha extendido como se esperaba.

II. La Ley Especial Contra Delitos Informáticos

En el artículo 2° de la Ley Especial Contra Delitos Informáticos, se establecen una serie de definiciones, indicando que debe entenderse, a los efectos de esa Ley, por: tecnologías de información, sistema, data (datos), información, documento, computador, hardware, firmware, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña (password) y mensaje de datos.

Prevé esta Ley cinco (5) modalidades o categorías de delitos, según el bien jurídico que resulte afectado, que pueden ser: a) contra los sistemas que utilizan tecnologías de información; b) contra la propiedad; c) contra la privacidad de las personas y de las comunicaciones; d) contra niños, niñas o adolescentes; y e) contra el orden económico. Tipificando así las siguientes conductas o actos:

Dentro de los delitos **contra los sistemas que utilizan tecnologías de información**, encontramos: 1) el **acceso indebido** a un sistema, 2) el **sabotaje o daño intencional a sistemas**, 3) el **sabotaje o daño culposo** a sistema, 4) el **acceso indebido o sabotaje a sistema protegido**, 5) la **posesión de equipos o prestación de servicios de sabotaje** a sistemas, 6) el **espionaje informático** y 7) la **falsificación de documentos** que se encuentren incorporados a un sistema. Las penas de prisión oscilan entre 1 a 8 años y todos los delitos prevén multas, así como, en algunos casos, aumentos de pena cuando se ponga en peligro la seguridad del Estado o cuando el agente hubiera actuado con el fin de procurar obtener algún tipo de beneficio, para sí o para otro.

Entre los delitos **contra la propiedad**, establecidos en esta Ley especial, se encuentran: 1) el **hurto**, apoderamiento o sustracción de bienes o valores tangibles e intangibles de carácter patrimonial, contenidos en un sistema informático o medio de comunicación, para procurarse un provecho económico para sí o para otro; 2) el **fraude** al insertar instrucciones falsas o fraudulentas en un sistema, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno; 3) la **obtención indebida de bienes o servicios**, al utilizar una tarjeta inteligente ajena o algún instrumento destinado a los mismos fines, para proveer un pago, sin la autorización debida; 4) el **manejo fraudulento de tarjetas inteligentes o instrumentos análogos**, al crear, grabar, copiar, alterar, duplicar o eliminar data o información, contenida en alguna tarjeta inteligente o en cualquier otro instrumento destinado a los mismos fines. En la misma pena incurrirá quien adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de esas tarjetas; 5) la **apropiación de tarjetas inteligentes o instrumentos análogos**, que se hayan perdido, extraviado o entregado por equivocación a otra persona, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta al usuario autorizado o a la entidad emisora; 6) la **provisión indebida de bienes o servicios**, así como de dinero o valores, por parte de quien tiene conocimiento que la tarjeta inteligente se encuentra vencida, ha sido revocada, haya sido indebidamente obtenida o retenida, sea falsificada o alterada; y 7) la **posesión de equipo para falsificaciones** de tarjetas inteligentes o instrumentos análogos, por parte de persona que no está autorizada para emitir o fabricar los mismos. Las penas de prisión oscilan entre 1 a 7 años y todos los delitos prevén adicionalmente penas de multa.

En relación con los delitos **contra la privacidad de las personas y de las comunicaciones**, se tipifican los siguientes delitos: 1) la **violación de la privacidad de la data o información de carácter personal**, apoderándose, utilizando, modificando o eliminando por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otra persona. Se incrementará la pena si resultare un perjuicio para el titular de la data o información, o para un tercero; 2) la **violación de la privacidad de las comunicaciones**, al acceder, interceptar, interferir o reproducir, cualquier mensaje de datos o comunicación ajena; 3) la **revelación indebida de data o información de carácter personal**, obtenida mediante la violación de la privaci-

dad de la data de las personas o de las comunicaciones, sea en relación con ciertos hechos, imágenes, audios o información de carácter personal o íntimo. Se aumentará la pena si el hecho se realiza con fines de lucro. Las penas de prisión fluctúan de 2 a 6 años y todos estos delitos prevén adicionalmente penas de multa.

Con respecto a los delitos contra niños, niñas o adolescentes, esta Ley especial prevé dos modalidades: 1) la **difusión o exhibición de material pornográfico** o reservado a personas adultas, por cualquier medio que involucre el uso de tecnologías de información, y 2) la **exhibición pornográfica de niños o adolescentes**, utilizando la persona o la imagen de un niño, niña o adolescente, por cualquier medio que involucre el uso de tecnologías de información. El primer delito prevé pena de prisión de 2 a 6 años y el segundo delito de 4 a 8 años de prisión. Ambos delitos acarrean también penas de multa.

Finalmente, esta Ley prevé los siguientes delitos **contra el orden económico**: 1) la **apropiación de propiedad intelectual** de cualquier obra del intelecto, que haya obtenido mediante el acceso a cualquier sistema que utilice tecnología de información; y 2) la **oferta engañosa** que haga cualquier persona, que ofrezca bienes o servicios, mediante el uso de tecnologías de información, haciendo alegaciones falsas o atribuyéndole características inciertas a algún elemento de dicha oferta, de modo que pueda resultar algún perjuicio para el consumidor. Delitos estos que prevén penas de prisión de 1 a 5 años y multa.

III. Cuestionamientos a esta Ley Especial

A la Ley Especial Contra los Delitos Informáticos, se le han hecho muchos cuestionamientos, especialmente los siguientes: que establece delitos ya existentes en el Código Penal y en otras leyes especiales, como el hurto y el fraude, cuando la diferencia estriba casi exclusivamente en el medio empleado y en la naturaleza del bien jurídico afectado, pero eso es necesario para distinguirlos de los delitos tradicionales.

Que algunos de los términos y conceptos utilizados provienen del idioma inglés, lo cual es muy cierto y también muy lógico, ya que en este mundo globalizado, la mayoría de ellos son originarios de ese idioma y así se han popularizado por todo el mundo, como whatsApp, twitter, Facebook, instagram, hardware, software, google, gmail, hotmail, yahoo, etc.

También se ha mencionado que en Venezuela se sigue descodificando el Código Penal, promulgando decenas de leyes especiales para todo, lo que es muy cierto y lamentable, y debería evitarse. Quizás eso sólo se logre resolver, cuando se elabore un nuevo Código Penal, que aglutine y comprenda todas las leyes penales que actualmente se encuentran dispersas, para así evitar repeticiones y hasta contradicciones entre dichas leyes, lo cual atenta contra la necesaria seguridad jurídica.

Se le cuestiona la técnica legislativa empleada y el hecho de que no hace referencia alguna sobre la Ley de Mensajes de Datos y Firmas Electrónicas, ni a las conductas consideradas delictivas en dicha Ley, y, además, que usa una terminología distinta a aquella, lo cual crea confusión e inseguridad jurídica. Todo eso es cierto, y en buena parte eso se explica, porque una se trata de una Ley discutida y aprobada por la Asamblea Nacional y la otra mediante un Decreto-Ley del Ejecutivo Nacional.

IV. Procedimiento establecido en el Código Adjetivo Penal venezolano

El Código Orgánico Procesal Penal venezolano, que fue promulgado el 23 de enero de 1998, pero que entró en vigencia plena el 1 de julio de 1999, con varias reformas desde entonces, consagra en el Título VI, del Régimen Probatorio, específicamente en la Sección Cuarta del Capítulo II, que se refiere a los Requisitos de la Actividad Probatoria, lo relativo a **la ocupación e interceptación de correspondencia y comunicaciones**. Así vemos que en el artículo 204, se establece que "*En el curso de la investigación de un hecho delictivo, el Ministerio Público, con autorización del Juez o Jueza de Control, podrá incautar la correspondencia y otros documentos que se presuman emanados del autor o autora del hecho punible o dirigidos por él o ella, y que puedan guardar relación con los hechos investigados. De igual modo, podrá imponer la incautación de documentos, títulos, valores y cantidades de dinero, disponibles en cuentas bancarias o en cajas de seguridad de los bancos o en poder de terceros, cuando existan fundamentos razonables para deducir que ellos guardan relación con el hecho delictivo investigado. En los supuestos previstos en este artículo, el órgano de policía de investigaciones penales, en casos de necesidad y urgencia, podrá solicitar directamente al Juez o Jueza de Control la respectiva orden, previa autorización, por cualquier medio, del Ministerio Público, la cual deberá constar en la solicitud*".

En este mismo sentido, el artículo 205 *eiusdem*, en relación con la **interceptación o grabación de comunicaciones privadas**, dispone lo siguiente: "*Podrá disponerse igualmente, conforme a la ley, la inter-*

ceptación o grabación de comunicaciones privadas, sean éstas ambientales, telefónicas o realizadas por cualquier otro medio, cuyo contenido se transcribirá y agregará a las actuaciones. Se conservarán las fuentes originales de grabación, asegurando su inalterabilidad y su posterior identificación. A los efectos del presente artículo, se entienden por comunicaciones ambientales aquellas que se realizan personalmente o en forma directa, sin ningún instrumento o dispositivo de que se valgan los interlocutores o interlocutoras".

Ahora bien, **para poder realizar dichas intercepciones o grabaciones de comunicaciones privadas, el Código Orgánico Procesal Penal exige la autorización judicial de las mismas**. Así vemos que en el artículo 206, se señala que "*En los casos señalados en el artículo anterior, el Ministerio Público, solicitará razonadamente al Juez o Jueza de Control del lugar donde se realizará la intervención, la correspondiente autorización con expreso señalamiento del delito que se investiga, el tiempo de duración, que no excederá de treinta días, los medios técnicos a ser empleados y el sitio o lugar desde donde se efectuará. Podrán acordarse prórrogas sucesivas mediante el mismo procedimiento y por lapsos iguales, medios, lugares y demás extremos pertinentes. El órgano de policía de investigaciones penales, en casos de necesidad y urgencia, que deberán ser debidamente justificados, podrá solicitar directamente al Juez o Jueza de Control la respectiva orden, previa autorización, por cualquier medio, del Ministerio Público, que deberá constar en la solicitud, en la cual, además, se harán los señalamientos a que se contrae el aparte anterior. La decisión del Juez o Jueza que acuerde la intervención, deberá ser motivada y en la misma se harán constar todos los extremos de este artículo*".

Finalmente, el Código Adjetivo Penal también establece en el artículo 207, que "*Toda grabación autorizada conforme a lo previsto en este Código y en leyes especiales, será de uso exclusivo de las autoridades encargadas de la investigación y enjuiciamiento, quedando en consecuencia prohibido divulgar la información obtenida*".

V. Conclusiones

Es evidente que los objetivos establecidos en la Ley Especial no se han conseguido, ni se vislumbra que se vayan a respetar. Las conversaciones y comunicaciones privadas no están realmente protegidas en Venezuela, y cualquiera graba impunemente a otro, especialmente el gobierno, que tiene todo el poder, los equipos y los medios para hacerlo, y de hecho lo hace sin siquiera esconderlo, y los más altos funcionarios así lo reconocen públicamente, sin que eso les acarreé problema alguno. Por otro lado, es muy común la comercialización de la información de muchos usuarios, sin su autorización, la cual se le facilita a empresas que están buscando posibles nuevos clientes.

La afectación del derecho a la intimidad sólo puede permitirse y verse comprometido, excepcionalmente, por investigaciones penales serias y bien fundamentadas, para las cuales se requiere orden judicial, no únicamente Fiscal. En una investigación criminal se puede requerir la obtención de algunos archivos electrónicos, bien sea de mensajes de texto, de voz, por correos electrónicos, celulares, whatsApp, instagram o facebook u otras vías o redes sociales similares. Pero esa información debe restringirse a la absolutamente necesaria para la investigación, que normalmente es mínima.

Quizás se podría intentar establecer en Venezuela, en relación con delitos electrónicos o informáticos menos graves, algo similar a la Ley Hadopi, aprobada por el Senado francés en mayo de 2009, la cual establece que la primera vez que se detecte a alguien descargando películas o música ilegalmente, recibirá un correo electrónico como primer aviso o advertencia. De reincidir, recibirá entonces una segunda advertencia, intimándolo a no continuar con esa práctica ilícita. De persistir, se le podrá suspender el servicio de internet y hasta la desconexión permanente.

En relación con los cybercrimes, la tendencia es el llegar a acuerdos internacionales para adoptar acciones preventivas y represivas más eficientes, para combatir los delitos y las ofensas a través de la Internet.

Considero que se debe preservar en lo posible la garantía constitucional del libre acceso a la Internet, ya que esa es una herramienta muy importante y necesaria para la investigación y el desarrollo de los pueblos. Por ello, a pesar de todas sus deficiencias, es importante la existencia de esta Ley Especial y de otras que vendrán, como un paso más en la consecución de una verdadera protección a la privacidad, a la intimidad y al respeto por las comunicaciones entre las personas, ya que es necesario garantizar esos derechos humanos primordiales, que actualmente no se están protegiendo.

No se puede permitir, que con la excusa de una supuesta lucha contra un presunto terrorismo en Venezuela, que realmente no existe como tal, se pretenda controlar a la población y convertir al Estado en un gendarme, como ya se ha intentado a través de la llamada Ley Resorte, de Responsabilidad Social de Radio y Televisión, y muy especialmente mediante su reforma[5],

extendiendo sus controles a los servicios de internet y demás medios electrónicos, pretendiendo así limitar y restringir las transmisiones de información entre usuarios de la Internet y el contenido de los mismos, así como los foros y comentarios entre ellos, tratando de evitar que se hable de ciertos temas, como ya antes sucedió en relación con el precio del dólar. No sólo en sitios web, sino también en las redes sociales, como twitter y facebook. Si examinamos las disposiciones que últimamente ha dictado CONATEL, observaremos un listado casi interminable de prohibiciones, lo cual atenta contra la libertad de expresión y de información.

Algunos ciudadanos han sido procesados y condenados a penas de cárcel, por enviar mensajes de texto o publicar sucesos en redes sociales, e incluso por simplemente criticar al gobierno. Llegándose hasta el extremo de indicar que el doble sentido está prohibido. Evidentemente que esto es claramente censura, lo cual está prohibido por la Constitución.

Notas

1 Gaceta Oficial No. 37.313.
2 Gaceta Oficial No. 34.863.
3 Gaceta Oficial No. 37.148 del 28 de febrero de 2001.
4 Gaceta Oficial No. 38.086.
5 La llamada Ley Resorte fue parcialmente reformada en fecha 22 de diciembre de 2010, Gaceta Oficial No. 39.579, y reimpresa por error material en la Gaceta Oficial No. 39.610, del 7 de febrero de 2011.

1. REVISTA PENAL publica artículos que deben ser el resultado de una investigación científica original sobre temas relacionados con las ciencias penales en sentido amplio; ello incluye investigaciones sobre la parte general y la parte especial del Derecho Penal, el proceso penal, la política criminal y otros aspectos afines a estas disciplinas que preferentemente puedan ser extrapolables a otros países. Los artículos no deben haber sido publicados con anterioridad en otra revista.
2. Los trabajos deben enviarse por correo electrónico en formato Microsoft Word (o en su defecto, en formato *.txt) a la dirección: jcferreolive@gmail.com
3. La primera página del documento incluirá el título del trabajo en castellano y en inglés, el nombre completo del autor o los autores, su adscripción institucional y su correo electrónico, el sumario, un resumen analítico en castellano y en inglés (de unas 100 palabras aproximadamente) y palabras clave en castellano y en inglés (entre 2 y 5 palabras)
4. Los autores deberán elaborar las referencias bibliográficas conforme a las normas ISO 690.
5. Los trabajos se someterán a la evaluación de al menos dos árbitros externos siguiendo el sistema de evaluación doble ciego. Los autores recibirán información del eventual rechazo de sus trabajos, de las reformas requeridas para la aceptación definitiva o de dicha aceptación. Los originales aceptados se publicarán en el primer volumen con disponibilidad de páginas.
6. Es condición para la publicación que el autor o autores ceda(n) a la Revista, en exclusiva, los derechos de reproducción. Si se producen peticiones del autor o de terceros para reproducir o traducir artículos o partes de los mismos, la decisión corresponderá al Consejo de Redacción. Se deberá indicar que el artículo ha sido publicado previamente en el correspondiente número de Revista Penal.

Apuesta por Tirant Online, la base de datos jurídica de la editorial más prestigiosa de España.*

www.tirantonline.com

Suscríbete a nuestro servicio de base de datos jurídica y tendrás acceso a todos los documentos de Legislación, Doctrina, Jurisprudencia, Formularios, Esquemas, Consultas o Voces, y a muchas herramientas útiles para el jurista:

- Biblioteca Virtual
- Herramientas Salariales
- Calculadoras de tasas y pensiones
- Tirant TV
- Personalización
- Foros y Consultoría
- Revistas Jurídicas
- Gestión de despachos
- Biblioteca GPS
- Ayudas y subvenciones
- Novedades

* Según ranking del CSIC

96 369 17 28

96 369 41 51

atencionalcliente@tirantonline.com

www.tirantonline.com