UNIVERSIDAD FASTA

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA

Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática

CIIDDI – 2014

Sede: Mar del Plata

Trabajo:

Problemáticas en torno a la investigación de los delitos informáticos

Autora:

Sabrina B. Lamperti*

* Abogada (2007 - UNMDP) – Especialista en Criminalidad Económica (2012 – Universidad Castilla-La Mancha / UNMDP) – Integrante de la Unidad Funcional de Instrucción y Juicio Nº 10 de Delitos Económicos del Departamento Judicial Mar del Plata.

Problemáticas en torno a la investigación de los delitos informáticos

A la hora de abordar las investigaciones vinculadas a delitos informáticos, quienes desarrollamos la labor investigativa nos enfrentamos a problemas que no siempre son fáciles de resolver, no siendo tampoco uniformes las soluciones adoptadas. Existen diversos obstáculos que impiden la investigación eficaz de la delincuencia y el enjuiciamiento penal de los "delincuentes informáticos". Obstáculos como fronteras jurisdiccionales, insuficiente capacidad para compartir los datos de la investigación, dificultades técnicas para rastrear los orígenes de los ciberdelincuentes, disparidad de capacidades de investigación y capacidades forenses, escasez de personal bien preparado y una cooperación errática con otras partes responsables de la seguridad electrónica, son algunas de las cuestiones a tratar.

Básicamente, podemos resumirlas en tres grupos: I. Lo que atañe a la tipificación de conductas delictivas; II. La faz del derecho procesal; III. La cuestión relativa a la jurisdicción y competencia. Asimismo advertimos otros casos que, de momento, no tienen una solución legislativa.

Seguidamente realizaremos una aproximación a las problemáticas que se suscitan y algunas posibles soluciones.

I. Tipificación de las conductas delictivas

En lo atinente a los delitos tradicionales, la decisión de uno o unos cuantos países de tipificar como delito ciertas conductas, puede influir en la capacidad de los delincuentes para actuar en dichos países. Con todo, cuando se trata de delitos relacionados con Internet, la capacidad de influencia sobre los delincuentes de un solo país es mucho más reducida, ya que éstos actúan conectándose a la red a partir de cualquier lugar. El fracaso de las investigaciones internacionales y de las peticiones de extradición es un fenómeno muy frecuente cuando los delincuentes actúan a partir de países que no tipifican como delito sus conductas.

La cooperación oportuna y eficaz entre los países es fundamental para garantizar el éxito de una investigación porque, a diferencia de la investigación tradicional, es muy corto el tiempo de que dispone un investigador de delitos cibernéticos. Aunque ya se han concertado algunos acuerdos de asistencia judicial recíproca, el establecimiento de procedimientos de respuesta rápida y la cooperación internacional resultan indispensables.

Uno de los primeros intentos lo realizó el Comité Europeo para los Problemas de la Delincuencia, órgano dependiente del Consejo de Europa dentro del marco de la Unión Europea, el cual elaboró un convenio preliminar sobre delitos informáticos en la reunión del 25 de mayo de 2001, realizada en Estrasburgo.[1]

Unos meses después, el 23 de noviembre de 2001, se realizó una nueva reunión del Consejo de Europa en la ciudad de Budapest, Hungría, en la cual tanto países europeos como de

1 Hocsman, Heriberto Simón; *Negocios en internet*; Edit. Astrea; 2005, pág. 259.

otros países adheridos establecieron el ***Convenio de Cibercriminalidad***[2], entendiendo que debían ponerse de acuerdo sobre algunas cuestiones básicas de la política penal de cada país participante, con miras a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional.

Los principales objetivos del Convenio apuntan a la introducción de conductas tipificadas y a la coordinación y cooperación entre las policías y administraciones de los países que se adhieran a éste.

En primer término se precisaron algunas cuestiones terminológicas, relativas a las definiciones de: sistema informático, datos informáticos, prestador de servicio y datos de tráfico.

Posteriormente trataron cuestiones relativas al derecho material y el derecho procesal. Dentro de las disposiciones de ***derecho material*****,** los delitos informáticos son clasificados en la Convención como:

1) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos *(acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad del sistema y abuso de equipos e instrumentos técnicos)*

2) Infracciones informáticas *(falsedad informática y estafa informática)*

3) Delitos vinculados al contenido *(se dirige a tipificar las Infracciones relativas a la pornografía infantil).*

4) Delitos vinculados a violación de la propiedad intelectual y otros derechos afines. *(se intenta legislar acerca de los atentados a la propiedad intelectual definida por la legislación de cada Estado, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático).*

Otro de los esfuerzos por aunar criterios uniformes en todo el mundo, es realizado desde la sede de la ***Organización de Naciones Unidas***, a través de las reuniones que se celebran con frecuencia en el seno de dicha organización, y en especial de los Congresos sobre Prevención del Delito y Justicia Penal, en donde se ha tomado este tópico como un desafío en el cual avanzar.

Según el documento elaborado en el marco del ***Undécimo Congreso sobre Prevención del Delito y Justicia Penal***[3] las formas delictivas halladas serían:

1) Aquellos delitos informáticos que atacan a las **propias tecnologías de la información y las comunicaciones**, y a los que algunas veces se hace referencia como delitos contra la confidencialidad, la integridad o la disponibilidad de sistemas de computadoras. Éstos incluyen formas de robo de servicios de telecomunicación y robo de servicios de computación utilizando diversas técnicas de piratería (según la tecnología, estos incluyen acceso no autorizado, robo de códigos y contraseñas, clonación digital, robo de la información contenida en la banda magnética de la tarjeta de crédito -*skimming*- y otros). Los servidores y los sitios web pueden ser blancos de ataques de servicios. En algunos casos, esos delitos son el resultado de los ataques distribuidos

2 Versión online disponible en: http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm. Accesible: marzo de 2014.

3 ONU; Undécimo Congreso sobre Prevención de Delito y Justicia Penal – 18 al 25 de abril de 2005 en Bangkok, Tailandia; A/CONF: 203/14.

de denegación de servicio en que docenas o cientos de computadoras comprometidas se utilizan como “zombies” para bombardear el blanco escogido con peticiones tan numerosas que no se puede atender a ninguna.

2) Delitos que emplean a las computadoras como **instrumentos o medios** para cometerlos. Hay sitios web dedicados al “*carding*” (falsificación de tarjetas de crédito), que incluye la producción de moneda falsificada de gran calidad y pasaportes. El robo de datos abarca un espectro amplio, desde la piratería de información y el espionaje industrial hasta la transgresión de derechos de autor (robo de propiedad intelectual en forma de programas informáticos pirata, ficheros de música, vídeo digital y otros). El robo de datos quizá no sea sencillamente un delito económico; también puede violar la privacidad y los derechos conexos del individuo en los nuevos delitos asociados con el robo de la identidad.

3) Delitos **clásicos de defraudaciones** pero relacionados con las computadoras, incluidos el robo económico, como los ataques de piratería contra bancos o sistemas financieros, o el fraude, incluida la transferencia electrónica de fondos. También se han expresado inquietudes con respecto al blanqueo electrónico de capitales y evasión tributaria. Las computadoras también se utilizan para facilitar una gama amplia de ventas telefónicas y fraude de inversiones con prácticas engañosas. Entre estos delitos encontramos: la “pesca” de información o “*phishing*” al igual que la basura informática (spam), el fraude de títulos, asociado con la manipulación en la bolsa de valores de inversiones de valor bajo, es todavía relativamente raro a nivel de los consumidores.

4) Otros delitos **ya tipificados**, como la extorsión (amenaza de divulgar información comercial o personal o dañar datos o sistemas), el acoso y casos de difamación o calumnia, que también se realizan en línea.

5) Hay una variedad de delitos relacionados con el **contenido** -y en los que se emplean computadoras-, en particular la difusión de material ilícito y nocivo y que apunta particularmente al problema de la pornografía infantil, dado que desde fines del decenio de 1980 ha habido una tendencia creciente a distribuir pornografía infantil mediante una diversidad de redes de computadoras, utilizando diversos servicios de Internet, incluidos los sitios web, los grupos de noticias Usenet, los sistemas de conversación IRC, y las redes entre pares (P2P)[4]. Estas redes se han utilizado para facilitar intercambios de información, comerciar en imágenes o vídeos de pornografía infantil, realizar transacciones monetarias y trasmitir información con respecto al turismo sexual infantil. Una cierta proporción de la distribución de pornografía infantil tiene fines comerciales (más que de intercambio no monetario entre pedófilos) y está vinculada a la delincuencia organizada transnacional. La Internet se ha utilizado también para otros delitos de contenido, como la distribución de propaganda de material motivado por los prejuicios y la xenofobia

6) Relacionados a **otros delitos transnacionales**, como la vinculación dada entre el

4 Aunque en la actualidad estén en desuso tanto UseNet como el servicio de chat IRC a los fines de la distribución de pornografía infantil, siendo mayormente utilizadas las nuevas redes sociales (Facebook, Youtube, entre otros) o bien el intercambio a través de servicios P2P (E-Mule, Ares, etc.)

terrorismo y la Internet. Hay indicios de que Internet se utiliza para facilitar la financiación del terrorismo y como instrumento logístico para planificar y ejecutar actos de terrorismo. Esas actividades son distintas del terrorismo cibernético, que ha sido definido por el Centro Nacional de Protección de la Infraestructura de los Estados Unidos como un "acto delictivo perpetrado con el uso de computadoras que resulta en violencia, muerte y/o destrucción, y que crea terror con el propósito de ejercer presión sobre un gobierno para que cambie sus políticas".

No caben dudas que el derecho sustantivo de cada país debe ser adecuado para la correcta persecución de esta clase de delitos. En este sentido consideramos que sería importante la adhesión y posterior ratificación por parte de todos los países, de un instrumento como el Convenio de Cibercriminalidad elaborado por el Consejo de Europa (Budapest, 2001); para luego incorporar a las legislaciones de cada Estado, las tipificaciones que resulten necesarias. Esta situación gravita radicalmente sobre el tema de la competencia judicial, dado que ésta se dirime en función de la calificación dada a un hecho.

II. Desde el derecho procesal

a) Materia probatoria:

Otro de los aspectos importantes a tener en cuenta lo constituye el de la prueba de los hechos investigados. Como nos ilustra el Dr. Riquert, *"las dificultades que se producen en materia probatoria en el proceso penal, es una de las cuestiones que deberán preverse de lege ferenda, ya que no bastará el adecuar la legislación de fondo si la de forma permanece atada al pasado. Las dudas que genera la denominada "prueba informática", su validación o equiparación a la "prueba documental", son temas sobre los que los procesalistas deberán reflexionar seriamente a efectos de no frustrar la ley sustantiva y, a la vez, no atentar contra las garantías constitucionales"*[5].

Cuando se investigan delitos relacionados con las computadoras, hay que hacer frente a numerosos problemas forenses. Parte del problema de reconstruir un incidente en un caso de delito cibernético es que gran parte de las pruebas son intangibles y transitorias. En lugar de pruebas físicas, las investigaciones de delitos cibernéticos procuran encontrar rastros digitales que con frecuencia son inestables y de corta duración. Una de las razones de la inestabilidad es que algunos tipos de información sobre direcciones y rutas electrónicas (es decir, los "datos sobre el tráfico") no se almacenan de manera permanente. Esa información puede quedar sólo en la memoria de un sistema de computadoras por un período corto y luego se le superpone otra ruta de información.[6]

b) Capacitación de operadores judiciales:

No es tampoco una cuestión menor lo relacionado con la capacitación de los agentes de justicia, ya que el conocimiento específico requerido para la promoción de la investigación tiene vital trascendencia con la resolución positiva del caso. En este sentido, se cuenta siempre con

5 Riquert, Marcelo A; *Informática y derecho penal argentino*; Edit. Ad Hoc, 1999, pág. 82.
6 ONU; *Undécimo Congreso...*; Op.Cit.; pág. 12.

asesoramiento de ingenieros en informática que orientan a los operadores judiciales acerca de cómo implementar ciertas medidas investigativas tendientes a la dilucidación de los hechos denunciados.

Sin perjuicio de ello, es de resaltar que -en materia de pericias informáticas- no existe aún un proceso o método científico establecido que garantice el correcto accionar. En este aspecto debemos recordar que *"las ciencias forenses deben cumplir con tres principios básicos: evitar la contaminación, actuar metódicamente y controlar la cadena de evidencia. El método es el que permite garantizar el trabajo realizado, su confrontación en un juicio oral, de ser necesario, y la trazabilidad. Por las características propias de las tecnologías de la información y la comunicación, su gran dinamismo y diversidad, era necesario contar con algún proceso que sea lo suficientemente amplio, como para adaptarse a cualquier tecnología, y a su vez, tuviera guías concretas de implementación en plataformas específicas con herramientas actuales y a disposición."*[7]

c) Medios de almacenamiento:

Pero más allá de la cuestión técnica acerca del modo de incorporación de la prueba obtenida para la demostración de un ilícito, advertimos otra cuestión no menos importante y que tiene que ver con el medio en que se almacena la información y lo relativo a la solicitud de medidas cautelares sobre ésta, en particular en cuanto a la competencia del órgano jurisdiccional interviniente.

Esto es así, porque no podemos dejar de tener en cuenta, que muchas empresas y personas hoy en día no almacenan la información en los discos rígidos de las computadoras que utilizan, sino que lo hacen en "la nube". El término técnico es "cloud computing" (en español: computación en la nube), y se refiere al sistema que permite ofrecer servicios de computación a través de Internet; tales como los que ofrece Google a través de Google Drive (antes Gdocs), Dropbox, y SkyDrive (de Microsoft), -por nombrar algunos de los más conocidos-.

El *cloud computing* permite que: a) la información ya no tenga que almacenarse necesariamente en los dispositivos informáticos de los individuos o de empresas, sino en los sistemas proporcionados por la "nube", no siendo ya necesario instalar aplicaciones informáticas, sino que éstas se ejecutarán online a través de Internet; b) La puesta a disposición de los usuarios de infraestructuras tecnológicas a través de Internet, de modo que recursos informáticos dispuestos en red sean compartidos por varios usuarios y a través de distintos dispositivos, pudiendo trabar conjuntamente sobre el mismo contenido.[8]

De este modo se advierten los aspectos controvertidos desde el punto de vista del sistema jurídico y que guardan relación con: la posibilidad de acceso desde cualquier parte a un documento o servicio, para ser trabajado en línea, y la conservación de los datos que se

7 Di Iorio, Ana Haydeé – Greco, Fernando y otros; *"La recuperación de la información y la informática forense: una propuesta de proceso unificado";* trabajo en formato PDF presentado por los autores en el marco del I Congreso Argentino de Ingeniería. 8, 9 y 10 de agosto de 2012, Mar del Plata, Argentina.

8 Observatorio Regional de Sociedad de la Información (ORSI) y el Consejo Regional Cámaras de Comercio e Industria de Castilla y León; *"Cloud Computing: La tecnología como servicio".* Pág. 13. Disponible en: http://issuu.com/orsicyl/docs/cloud_computing?mode=a_p Pág. 10. Accesible: marzo de 2014.

almacenan en manos de un tercero.

Los interrogantes, en consecuencia, surgen palmariamente: ¿Qué sucedería en caso de solicitar al juez que intervenga en el conocimiento de un hecho ilícito cometido a través de medios informáticos, la posibilidad del "allanamiento y secuestro" de dicha información?. ¿Cómo determinar el grado de responsabilidad de cada usuario frente a un hecho ilícito si se encuentran en distintas jurisdicciones? La respuesta no es sencilla ni se ha encontrado una solución unívoca.

En el documento elaborado en el marco del Undécimo Congreso de las Naciones Unidas sobre Prevención de Delito y Justicia Penal, se ha dicho que: *"La investigación y el enjuiciamiento efectivos de los delitos relacionados con las computadoras suelen requerir el rastreo de la actividad delictiva a través de una diversidad de proveedores de servicios de Internet o compañías con computadoras conectadas a la Internet. Para lograr el éxito, los investigadores deben seguir la pista de las comunicaciones hasta la fuente y las computadoras u otros dispositivos afectados, trabajando con proveedores de servicios intermedios en diferentes países. (...)* ***Cuando los proveedores están situados fuera de la jurisdicción territorial del investigador, como suele ser el caso, los organismos de represión necesitan ayuda de sus contrapartes de otras jurisdicciones.*** *Las medidas tradicionales de asistencia judicial recíproca, y aun las medidas más expeditivas, están previstas normalmente para obtener datos históricos y en tiempo real de casos en que están involucrados sólo dos países (por ejemplo, el país de la víctima y el país del delincuente). Cuando el delincuente encamina comunicaciones a través de tres, cuatro o cinco países, el proceso de asistencia judicial requiere períodos sucesivos antes de que los organismos de represión puedan obtener datos de cada uno de los proveedores de servicios en la etapa siguiente de la pista de las comunicaciones, con lo que aumenta la posibilidad de que los datos no estén disponibles o se hayan perdido, y de que el delincuente permanezca encubierto y en libertad para cometer nuevos actos delictivos*.[9] (El resaltado me pertenece).

Para hacer frente a estas vicisitudes algunos especialistas han propuesto la posibilidad de implementar **"software judicial a distancia"**.[10] Sus posibles funciones serían las siguientes:

• Función de registro: Esta función permitiría que los organismos competentes registraran contenidos ilegales y compilaran información sobre los ficheros almacenados en el ordenador.

• Grabación: Los investigadores podrían grabar datos tratados en el sistema informático del sospechoso pero no almacenados permanentemente. Si, por ejemplo, el sospechoso utiliza servicios de voz por IP para comunicar con otros sospechosos, normalmente no se almacena el contenido de las conversaciones. El software judicial a distancia podría grabar los datos procesados y conservarlos para que los pudieran consultar los investigadores.

• Registrador de teclas: Si el software judicial a distancia contiene un módulo que registra los golpes de tecla, se podría utilizar para registrar las contraseñas que utiliza el sospechoso para

9 ONU; 11º Congreso...; *Op.Cit.*, pág. 14.

10 Unión Internacional de Comunicaciones; *El Ciberdelito: Guía para los países en desarrollo"*. Documento elaborado por la División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias, sector de Desarrollo de las Telecomunicaciones de la UIT. Abril de 2009. Accesible: marzo de 2014. Disponible en: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf ; pág. 215.

cifrar sus archivos.

• Identificación: Con esta función los investigadores podrían demostrar la participación del sospechoso en un delito, aún si utiliza servicios de comunicación anónimos que impiden que los investigadores identifiquen al infractor siguiendo el rastro de la dirección IP utilizada.

• Activación de periféricos: El software se podría utilizar a distancia para activar una webcam o el micrófono para observar el recinto. Si bien las posibles funciones del software parecen muy útiles para los investigadores, se ha de señalar que la utilización de ese software plantea diversas dificultades jurídicas y técnicas. Como por ejemplo, dificultades de instalación habida cuenta de las medidas de protección de que disponen la mayoría de los ordenadores, tales como buscadores de virus y cortafuegos, todos los métodos de instalación a distancia plantean dificultades a los investigadores. Además, el software judicial a distancia sólo permitiría analizar sistemas informáticos que están conectados a Internet y, por otra parte, es difícil mantener la integridad del sistema informático del sospechoso. En lo que respecta a estas últimas consideraciones, por lo general el software judicial a distancia no puede reemplazar su examen físico. Antes de llevar a efecto una disposición que autoriza a los investigadores a instalar este tipo de aplicaciones, también se han de tener en cuenta varios aspectos jurídicos. Las garantías que contienen las constituciones de muchos países y los códigos de derecho penal, limitan las funciones que puede tener ese software. Además de las consideraciones meramente nacionales, la instalación de software judicial a distancia podría violar el principio de soberanía nacional. Si el software es instalado en un ordenador portátil que sale del país después de su instalación, éste podría ser objeto de trabajo de los investigadores y estaría llevándose a cabo investigaciones judiciales en un país extranjero sin haber recibido permiso de las autoridades competentes.

Aunque todas estas herramientas sean técnicamente implementables quedará analizar si, a la luz de los principios y garantías constitucionales y de derechos humanos suscriptos por nuestro País (art. 18, 19, y 75 inc. 22º de la Constitución Nacional), resulta posible su aplicación en nuestro marco jurídico.

También debe destacarse el avance realizado por la Organización de Estados Americanos[11] al implementar el Portal Interamericano de Cooperación en materia de Delitos Cibernéticos. En los objetivos descriptos en su sitio web, encontramos que fue creado para facilitar y hacer más eficiente la cooperación y el intercambio de información entre los expertos gubernamentales de los Estados miembros de la OEA con responsabilidades en materia de delito cibernético o en cooperación internacional en la investigación y persecución de este delito. Entre sus logros se destacan el establecimiento de la “Red 24/7 para Delitos de Alta Tecnología”[12], esto es, de actuación las 24 hs. los siete días de la semana, estableciendo puntos de contacto en los países participantes que requieran asistencia urgente con las investigaciones que involucran

11 Organización de los Estados Americanos, Secretaría de Asuntos Jurídicos. Departamento de Cooperación Jurídica. Disponible en:http://www.oas.org/juridico/spanish/cybersp.htm . Accesible en: marzo de 2014.

12 OEA, documento elaborado por Albert Rees de la Sección de Delitos Informáticos y Propiedad Intelectual División de lo Penal, para el Departamento de Justicia de los Estados Unidos . Accesible: marzo de 2014. Disponible en: http://www.oas.org/juridico/spanish/cyber_g8.htm

pruebas electrónicas. Participan de esta iniciativa cuarenta y ocho países, entre los que se encuentran: Brasil, Jamaica, Canadá, México, Chile y Perú.

Su modalidad de procedimiento apunta a la conservación de las pruebas electrónicas, tales como: correo electrónico, registros de chat e información de Instant Messenger, correo electrónico basado en la red, páginas web, datos guardados en computadoras, registros de usuarios. Así también respecto de los Proveedores de Servicio de Internet (ISP) para recolectar información sobre: conexión esencial a Internet, registros sobre los usuarios, información sobre la conexión, datos archivados. La necesidad de identificar puntos de contacto, permite dar intervención a la autoridad competente con experiencia informática, y el conocimiento de normas y procedimientos locales.

La Sección de Delitos Informáticos y Propiedad Intelectual (CCIPS) del Departamento de Justicia es el punto de contacto. Este CCIPS recibe la llamada identificando del solicitante la asistencia que busca, que puede consistir en: la preservación de los registros, el reporte de la actividad delictiva en línea en los Estados Unidos que esté afectando a la nación solicitante, o la clausura del sitio web, por ejemplo en los casos en que contengan pornografía infantil ó sean sitios destinados al *phishing.* El CCIPS determina si la solicitud implica una violación de las normas de los Estados Unidos, y en caso afirmativo contacta a las autoridades competentes apropiadas en dicho país. En ese caso, los agentes de la autoridad de los Estados Unidos trabajan con los agentes solicitantes para obtener las pruebas necesarias, siendo éstas obtenidas y compartidas informalmente entre agencias de la autoridad. Si en cambio ninguna norma de los Estados Unidos ha sido violada, el CCIPS puede contactar al ISP para solicitar la preservación de los registros o informar al país solicitante sobre los resultados de la solicitud de preservación.

Sin embargo, debe tenerse en cuenta que el proceso del 24/7 no importa la sustitución de los procedimientos formales tratándose solamente de un paso previo y necesario, tendiente a la cooperación judicial en materia de investigación para la preservación de la prueba más inmediata; por lo que debería complemetarse con una adecuada legislación procedimental de carácter internacional para una solución integral y respetuosa de los principios y garantías de las legislaciones internas de cada Estado.

También se presenta como viable la posibilidad de una comunicación más fluida con otros organismos estatales, interestatales e internacionales, a través de solicitudes por medio de correos electrónicos en los que se emplee la firma digital, de modo de dotar de veracidad tanto a la calidad del remitente como la del receptor de la información.

III. Cuestión relativa a la jurisdicción y competencia

Se impone la necesidad de una reestructuración de los conceptos clásicos en pos de asegurar que el derecho cubra todas las posibilidades delictivas que brindan las nuevas tecnologías al ciberdelincuente. La importancia de su delimitación *"surge de la gran facilidad de las comunicaciones, que permiten a los delincuentes trasladarse con rapidez de un país a otro.*

Por eso, junto a la afirmación de la territorialidad de la ley, se presentan estas dos cuestiones más: la manera de dar eficacia a la represión en caso de que el delincuente traspase los confines del Estado en que perpetró el delito, y el ejercicio de la penalidad en caso de delitos cometidos en el extranjero".[13]

Tradicionalmente ante los llamados "delitos a distancia", cada sistema penal nacional procuraba determinar su alcance espacial, regulando su ámbito de vigencia: extensión de la "jurisdicción" de la propia ley y órganos del Estado que la aplican. Asimismo, el ordenamiento jurídico penal suele disponer de medidas de cooperación con otros Estados para facilitar la represión internacional del delito.[14] A esto se lo denomina *derecho penal internacional*.[15]

Es necesario recordar los pilares en que se basa el ámbito espacial de validez de la ley penal, por resultar principios reguladores que deben tenerse en cuenta a la hora de resolver los casos conflictivos; sea porque se trata de hechos cometidos fuera del territorio del Estado pero cuyo resultado disvalioso se produce en éste, sea porque aunque se ejecute aquí el *íter criminis* haga que termine en otro, etcétera. Esos principios son: 1º) Territorialidad, 2º) Real o de defensa, 3º) Personalidad o Nacionalidad, 4º) Universalidad.

Una de las soluciones intentadas por la doctrina[16], apunta a la posibilidad de aplicar una solución similar a los delitos de piratería. Recordemos que esto deriva de la aplicación del principio de universalidad, cuando los delitos que se comenten se realizan en el territorio de un Estado pero sus efectos repercuten en otros (delitos *juris gentium*). Así, el delito de piratería ha determinado la colaboración internacional, porque ordinariamente se comente fuera del territorio de todo Estado, de modo que la aplicación de la ley de un lugar que no sea el del buque perjudicado es típicamente extraterritorial; importando castigar un delito común cometido fuera del ámbito normal de validez de la ley penal. La Argentina en el Tratado de Montevideo, art. 13, acepta precisamente esa norma de colaboración, que se traduce en la otorgación de competencia al país "en cuyo poder caigan los delincuentes".[17] El delito de piratería determina la competencia, aunque no sea ofendida la Nación a cuyo puerto el pirata haya ido a parar, y si otra nación lo procesa, la Argentina nada tiene que pedirle, salvo que haya pactado la extradición de los reos de piratería conforme a la nacionalidad del buque perjudicado (por ej.: tratados con Estados Unidos, art. 21 inc. 11; con Bélgica, art. 2º, inc. 19; con Inglaterra, art. 2º inc. 22, etc.).[18]

---

13 Jiménez de Asúa, Luis; *Tratado de Derecho Penal*, T.II, 2ª edición, Editorial Losada S.A., Buenos Aires, 1958; citado por D'Alessio, José (Dir); *Código Penal de la Nación comentado y anotado*; T.I, 2ª edición, Editorial La Ley, pág. 3.

14 Creus, Carlos; *Derecho Penal. Parte General*; 4ª edición, 1996, Edit. Astrea, Buenos Aires, pág. 108.

15 En el *derecho penal internacional*, los titulares de legislación son los Estados y las normas son de carácter interno de éstos, diferenciándose de esta forma del *derecho internacional penal*, el cual es una parte del derecho internacional público, y en el que es la comunidad internacional la que ostenta el carácter de legislador, siendo sus normas de carácter internacional, regulando delitos que afectan a la humanidad toda y no simplemente sobre los súbditos o intereses de un determinado Estado. Creus; Op.Cit.; pág. 108.

16 Sáez Capel; Apunte de disertación llevada a cabo en fecha 11/11/2011 en el marco del curso de Especialización de Criminalidad Económica, de la Universidad Castlla La Mancha-UNMDP.

17 Soler; Sebastián; *"Derecho penal argentino"*, Tipográfica Editora Argentina, Bs. As., 1963, T, III.; pág. 187.

18 Ibídem.

IV. Otros casos cuestionables.

Algunas cuestiones que resultan interesantes para su análisis por cuanto son generadoras de debate, principalmente por no advertirse soluciones visibles.

Una de ellas tiene que ver con la utilización de programas específicos que permiten la navegación anónima (TOR, PGP y FreeNet). La navegación a través de proxy, un servidor intermedio entre nuestra PC e Internet que sirve -dependiendo de la configuración del proxy- para proteger nuestra IP en los sitios en los que navegamos, es también causante de problemas. Ciertos servicios de Internet complican la tarea de identificar sospechosos. Las comunicaciones anónimas pueden ser únicamente un producto de un servicio u ofrecerse con la intención de evitar desventajas para el usuario. Entre estos servicios, cabe citar los siguientes: terminales públicos de Internet (por ejemplo, terminales en el aeropuerto, cibercafés ó el uso de la red de WI-FI pública o de terceros que ofrecen el servicio de internet a sus clientes), redes inalámbricas; servicios móviles de prepago que no requieren registro; capacidades de almacenamiento de páginas ofrecidas sin registro; servidores de comunicación anónimas, y repetidores de correo anónimo.[19]

Con lo que el intento de identificar al autor de un hecho ilícito que haya utilizado este tipo de conexión para valerse en la realización de una maniobra ilícita, se ve como imposible. Aquí es donde surge palmariamente la evolución de las tecnologías en detrimento del plano de lo jurídico. No siendo posible determinar por los medios comisivos de algún hecho ilícito, desde dónde se desarrolla la maniobra, deviene en una imposibilidad de la persecución penal.

Otra de las maniobras que puede generar algún conflicto de encuadre jurídico es la ciberocupación (cybersquatting, en inglés), que consiste en el registro de marcas o nombres ajenos como nombres de dominio, para luego reclamar una suma de dinero por la “restitución” de la dirección virtual. A simple vista, esta figura parecería tener cierta similitud con un acto extorsivo, no obstante lo cual ha entendido parte de la doctrina[20] en que no es factible incluirla dentro de la redacción de la conducta prohibida por el art. 168 del Código Penal[21]. Con lo que se entiende que aún no se encuentra tipificada esta maniobra en nuestra legislación penal; sin perjuicio de las medidas administrativas que se están tomando.[22]

Desde otro aspecto, también hemos visto que en los últimos tiempos son frecuentes los casos de “robo de identidad digital”, los cuales generan serias consecuencias para los afectados. La tipificación de este delito debería urgir para ser sancionadas las conductas de quienes emplean una identidad falsa con diferentes fines como quienes utilizan identidades falsas para hacerse

---

19 Unión Internacional de Telecomunicaciones; Op.Cit.; pág. 82/3.

20 Vibes, Federico Pablo; *“El nombre de dominio en Internet”*; Edit. La Ley, 2003, pág. 284.

21 En efecto, para la configuración de éste se exige la *“intimidación o simulación de la autoridad pública”* o la *“falsa orden”* de la misma, como medios para obligar a otro a entregar, enviar, depositar, o poner a disposición propia o de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos. Por otro lado, el art. 169 CP requiere que exista *“...amenaza de imputaciones contra el honor o de la violación de secretos...”* por parte de quien cometiere alguno de los hechos expresados en el artículo anterior. De igual manera, tampoco se encuentra un delito específico dentro de los delitos contra la libertad, siendo que la coacción (art. 149 bis CP) reprime con pena de prisión o reclusión a quien realice *“...amenazas con el propósito de obligar a otro a hacer, no hacer o tolerar algo contra su voluntad...”*.

22 Se advierte cierto interés estatal en encontrar una solución a esta nueva modalidad, viéndose también favorable que ésta se resuelva por vías administrativas previas al derecho penal el cual siempre es considerado como *ultima ratio* del derecho, tal la política que está llevando a cabo NIC.Ar, la entidad registradora de dominios en Argentina.

pasar por un amigo, un extorsionador para esconder sus propósitos y amenazar a su víctima desde el anonimato; o los casos de ciberbulliying o ciberacoso y los casos de grooming[23] . Por este motivo, se ve con agrado los intentos del legislador por contemplar estas conductas. En este sentido, pudimos encontrar el Proyecto de Ley, Expte. Nº 4643-D-2010 sobre robo de Identidad digital[24], y en el Anteproyecto de Código Penal elaborado por la Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (Decreto P.E.N. 678/12) , que preside el Dr. Raúl Zaffaroni, el cual penaliza la conducta dentro del delito de "acceso ilegítimo a la información"[25]

En suma, creemos que la temática abordada es compleja y que cualquier análisis legislativo que se haga implicará estar en contacto permanente con especialistas que brinden soluciones dada la complejidad de la materia. Aún lográndose reformas necesarias, será también imperioso realizar seguimientos permanentes, a fin que el derecho no permanezca demasiado atrasado respecto del avance de la ciencia, el cual día a día nos sorprende con sus cambios.

…....

Sabrina Bibiana Lamperti

23 Grooming: acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, al crearse una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él.

24 Incorporación del artículo 139 ter del Código Penal. *Articulo 1. Incorpórese el art. 139 ter. del Código penal que quedará redactado de la siguiente manera: "Será reprimido con prisión de 6 meses a 3 años el que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. La pena será de 2 a 6 años de prisión cuando el autor asumiera la identidad de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediare su consentimiento o sea funcionario público en ejercicio de sus funciones".* Accesible: marzo de 2014. Disponible en: http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=4643-D-2010

25 Artículo 123 inc. "Será penado con prisión de seis meses a dos años el que... f) Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio."

BIBLIOGRAFÍA CONSULTADA

Publicaciones impresas:

✔ Aboso, Gustavo. *"La aplicación de la ley penal en el espacio y el delito de difamación cometido mediante internet (a propósito del caso "Dow Jones & Company c. Gutnick" de la Corte Suprema australiana)"*, en La Ley online. 18/03/2003.

✔ Creus, Carlos; *Derecho Penal. Parte General*; 4ª edición, 1996, Edit. Astrea, Buenos Aires.

✔ Hocsman, Heriberto Simón; *Negocios en internet*; Edit. Astrea; 2005.

✔ Jiménez de Asúa, Luis; *Tratado de Derecho Penal*, T.II, 2ª edición, Editorial Losada S.A., Buenos Aires, 1958.

✔ Lilli, Alicia Raquel – Massa, María Amalia; *"Delitos informáticos"*; LL, t.1986-A-832/843.

✔ López Rey y Arrojo, M.; *Criminalidad y abuso de poder*; Madrid, 1983

✔ Mata y Martín, Ricardo M.; *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001.

✔ Magliona, Markovich, Claudio P. y López Medel, Macarena; *Delincuencia y fraude informático. Derecho comparado y Ley 19,223*, conclusión nº 8, Editorial Jurídica de Chile, Santiago, 1999.

✔ Riquert, Marcelo A.; *"Delincuencia informática en Argentina y el Mercosur"*; Edit. EDIAR, 1ª edición, 2009.

✔ Riquert, Marcelo A.; *Informática y Derecho Penal Argentino*; Edit. AD HOC; 1999

✔ Sáez Capel, José; *"Informática y delito"*; Edit. Proa XXI, 2ª edición, agosto 2001

✔ Soler, Sebastián; *"Derecho penal argentino"*, Tipográfica Editora Argentina, Bs. As., 1963, T, III.

✔ Tiedemann, K; "*Lecciones de derecho penal económico"*; Barcelona, 1993, pág. 33

✔ Tobares Catalá, Gabriel H.-Castro Argüello, Maximiliano J.; *"Delitos Informáticos"*, Edit. Advocatus, 2010.

✔ Vaninetti, Hugo Alfredo; *Aspectos jurídicos de Internet;* Librería editora platense; La Plata, 2010.

✔ Vibes, Federico Pablo; *"El nombre de dominio en Internet"*; Edit. La Ley, 2003,

✔ Zaffaroni, Eugenio Raúl – Alagia, Alejandro – Slokar, Alejandro; *Manual de Derecho Penal. Parte General*. Edit. EDIAR, 2ª edición, Buenos Aires, 2007

Documentos digitales:

✔ Aurelio López-Tarruella Martínez; "*Infracciones internacionales de derechos de autor"*. Trabajo en formato PDF. Accesible: abril 2014. Disponible en: http://www.uaipit.com/files/publicaciones/%2F1283764121_1273224021_AurelioLopezTarruellaInfraccionesDDAA.pdf

✔ Castells, Manuel; *"La era de la información, Tomo I, Economía, Sociedad y Cultura"*. Accesible: julio de 2012. Disponible en versión PDF: http://www.geocapacitacion.com.ar/geoweb/biblio/laera.pdf

✔ Castells, Manuel; *"La galaxia internet"*, Cap.3, Reflexiones sobre internet, empresa y sociedad, Ed. Areté, Barcelona, 2001

✔ Consejo de Europa - *Convenio de Cibercriminalidad* - Accesible en: abril 2014. Disponible en: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=ITA

✔ Consejo y Parlamento Europeo; *La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia*; /*COM/2012/0140 final*/. Accesible: abril 2014 . Disponible en el sitio EUR-LEX: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:ES:HTML*

✔ Congreso Nacional de Chile, Biblitoteca. Departamento de estudios, extensión y publicaciones. *Delitos informáticos en la legislación de España, Francia, Alemania e Italia;* DEPESEX/BCN/SERIE INFORMES -AÑO XIV, Santiago de Chile, Julio 2004. Accesible: abril 2014. Disponible en: http://www.bcn.cl/carpeta_temas/temas_portada.2005-10-20.2791530909/documentos_pdf.2005-10-20.6075210557/archivos_pdf.2005-10-20.6853274934/archivo1

✔ Cornell University Law School – Legal Information Institute – EEUU. Accesible: abril 2014. Disponible en: *http://www.law.cornell.edu/uscode/text/18/1030*

✔ Di Iorio, Ana Haydeé – Greco, Fernando y otros; *"La recuperación de la información y la informática forense: una propuesta de proceso unificado";* trabajo en formato PDF presentado por los autores en el marco del I Congreso Argentino de Ingeniería. 8, 9 y 10 de agosto de 2012, Mar del Plata, Argentina.

✔ Fernández Delpech, Horacio; *Delitos informaticos;* documento en formato PDF. Accesible: abril 2014. Disponible en: *http://www.hfernandezdelpech.com.ar/DELITOS INFORMATICOS.pdf*

✔ Gobierno de España, Boletín Oficial del Estado. Ministerio de la Presidencia. Disponible en: http://www.boe.es/buscar/doc.php?id=BOE-A-1995-24544. Accesible: abril 2014

✔ Mariani, Pablo Raúl; *"Nociones sobre delitos informáticos"*. Trabajo disponible en: http://www.mariani-abogados.com.ar/documentos/9/Delitos%20Informaticos.doc Accesible: abril 2014.

✔ Mc. Kenna, Regis; Tiempo Real, Temas, Buenos Aires, 1998. Introducción y capítulos 1 y 2, págs. 21-85 y capítulo 4, págs. 117-137. Trabajo disponible en formato PDF.

✔ Ministerio de Educación, Cultura y Deporte – Secretaría de Estado de Cultura del Gobierno de España – Fallo de la Cour de Cassation: Sisro, Mar. 5, 2002, Bull. civ. I.. Accesible en: abril 2014 Disponible en idioma francés: *http://www.mcu.es/propiedadInt/docs/MC/Boletin_N2.pdf*

✔ Naciones Unidas – Undécimo Congreso sobre Prevención de Delito y Justicia Penal, llevado a cabo entre los días 18 a 25 de abril de 2005 en Bangkok, Tailandia. Nomenclador de catálogo: A/CONF.203/14. Disponible en: http://www.un.org/spanish/events/11thcongress/documents.html (Original en inglés.). Accesible: abril 2014. Versión en español en: http://es.scribd.com/doc/7322640/MEDIDAS-PARA-COMBATIR-LOS-DELITOS-INFORMATICOS. Accesible: abril 2014.

✔ Naciones Unidas - Información proporcionada por el Centro de Información para las Naciones Unidas en México, en relación al Undécimo Congreso de de las Naciones Unidas sobre Prevención de

Delito y Justicia Penal, llevado a cabo entre los días 18 a 25 de abril de 2005 en Bangkok, Tailandia. Disponible en: http://www.cinu.org.mx/11congreso/pdf/hoja_informativa6.pdf. Accesible: abril 2014.

✔ Naciones Unidas - Conclusiones del XII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Salvador, Brasil, entre los días 12 al 19 de abril de 2010. Disponible: http://www.cinu.mx/XIICongresoONUPrevencionDelito/docs/delincuentes_ciberneticos.pdf Accesible: abril 2014.

✔ Observatorio Regional de Sociedad de la Información (ORSI) y el Consejo Regional Cámaras de Comercio e Industria de Castilla y León; *"Cloud Computing: La tecnología como servicio".* Accesible: abril 2014. Disponible en: *http://issuu.com/orsicyl/docs/cloud_computing?mode=a_p*

✔ OMPI - Convenio de Berna para la protección de las Obras Literarias y Artísticas. Disponible: *http://www.wipo.int/treaties/es/ip/berne/trtdocs_wo001.html* Accesible: abril 2014.

✔ Organización de Estados Americanos. Disponible en:

http://www.oas.org/juridico/spanish/cyb_ven_LEY%20ESP_CON_DELI_INFOR.pdf
http://www.oas.org/juridico/MLA/sp/per/sp_per_cod_pen.pdf
www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf
Links accesibles en abril 2014.

✔ Organización de los Estados Americanos, Secretaría de Asuntos Jurídicos. Departamento de Cooperación Jurídica. Disponible en: *http://www.oas.org/juridico/spanish/cybersp.htm* . Accesible en: abril 2014

✔ Organización de los Estados Americanos. Documento elaborado por Albert Rees de la Sección de Delitos Informáticos y Propiedad Intelectual División de lo Penal, para el Departamento de Justicia de los Estados Unidos. Disponible en: *http://www.oas.org/juridico/spanish/cyber_g8.htm* Accesible: abril 2014.

✔ Rifkin, Jeremy; *"La era del acceso"*; Capítulo 3: La economía ingrávida; Editorial Paidós. Disponible en formato PDF.

✔ Rifkin, Jeremy; *La era del acceso*, Capítulo 11: Los conectados y desconectados; edición digital. Disponible en formato PDF.

✔ Senado de la República de México. Disponible: http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=33585 Accesible: abril 2014.

✔ Sitio web *Altalex.* Disponible en: *http://www.altalex.com/index.php?idnot=36653* Accesible: abril 2014.

✔ Sitio web *"Delitos Informáticos".* Disponible en: http://delitosinformaticos.com/legislacion/chile.shtml Accesible: abril 2014.

✔ Sitio web del Honorable Congreso de la Nación Argentina. Accesible: abril 2014. Disponible en:

http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=4643-D-2010

✔ Sitio web de *"Informática Jurídica"*. Accesible: abril 2014. Disponible en *http://www.informatica-juridica.com/legislacion/alemania.asp*

✔ Sitio web *Infoleg*, del Ministerio de Economía de la Nación Argentina. Disponible en:

http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm Accesible: abril 2014.

✔ Sitio web *Legifrance. Le service public de la diffusion du droit.* Accesible: abril 2014. Disponible en: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719&dateTexte=20120806 http://legifrance.gouv.fr/telecharger_rtf.do?idTexte=JURITEXT000017627214&origine=juriJudi

✔ Sitio web *"Legislation.gov.uk"*. The National Archives. Web oficial de Reino Unido de Gran Bretaña. Disponible en: *http://www.legislation.gov.uk/* Accesible: abril 2014.

✔ Sitio Web *"Nic.Ar"*. Disponible en: *https://nic.ar/* Accesible: abril 2014.

✔ Sitio web *"Noticias Jurídicas".* Accesible: abril 2014. Disponible en: http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t7.html#a44

✔ Sitio web *"Seguridad de la información",* Accesible: abril 2014. Disponible en. *http://www.segu-info.com.ar/delitos/delitos.htm*

✔ Unión Internacional de Telecomunicaciones; *"El Ciberdelito: Guía para los países en desarrollo"*. Documento elaborado por la División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias, sector de Desarrollo de las Telecomunicaciones de la UIT. Abril de 2009. Accesible: abril 2014. Disponible en: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

✔ Universidad de Concepción de Chile, Contraloría Universitaria, Julio de 2007. Disponible en: http://www2.udec.cl/~contraloria/docs/materias/delitosinformaticos.pdf Accesible: abril 2014.

✔ Universidad Nacional Autónoma de México - Instituto de Investigaciones Jurídicas. Disponible en: *http://info4.juridicas.unam.mx/ijure/tcfed/8.htm*. Accesible: abril 2014.