Sección 4: Documento de reflexión y cuestionario *

André Klip

Grupo Nacional Argentino. Contribuyeron en el presente trabajo: Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.

(A) Objeto del cuestionario (ver Anexos 1 2)

Las preguntas de esta Sección tratan generalmente del "Ciberdelito". Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. *El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.*

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. André Klip por email: andre.klip@maastrichtuniversity.nl

(B) Cuestiones sobre la jurisdicción

(1)(a) ¿Cómo localiza su país el lugar de comisión de un delito cometido en el ciberespacio?.

En la mayoría de los casos a través del número de IP utilizado por el ordenador que se conecta a la red. En caso de enmascaramiento o adulteración de IP a través de último lugar de conexión del número de IP.

En términos jurídicos, la aplicación de la ley penal argentina prioritariamente se rige por el art. 1° del CP: por los delitos cometidos o cuyos efectos deban producirse en el territorio nacional o en lugares sometidos a nuestra jurisdicción. Por lo que tendríamos jurisdicción si el hecho se concreta aquí o sus efectos se producen en nuestro territorio aunque la acción haya sido desplegada fuera de nuestras fronteras.

(b) ¿Su legislación nacional considera necesario y posible localizar el lugar donde se encuentran la información y las pruebas? ¿Dónde está la información que se

* Atención: El texto que se publica constituye la última versión original del informe nacional enviado por el autor, sin revisión editorial por parte de la Revista.

Revue électronique de l'AIDP / Electronic Review of the IAPL / Revista electrónica de la AIDP (ISSN - 1993-2995), 2014, RH-1:1

puede encontrar en la web? ¿Se encuentra donde el ordenador del usuario está físicamente presente? ¿Allí donde el proveedor de la red tiene su sede (jurídica o de hecho)? ¿Qué proveedor? ¿O es el lugar de la persona que posibilitó la disponibilidad de los datos? Si estas preguntas no se consideran jurídicamente relevantes, por favor, indique por qué.

Nuestra legislación carece de ley procesal penal que trate este tema. No obstante saber donde se encuentra almacenada la información resulta indispensable en procesos que involucran prueba digital.

En la mayoría de los casos se procede al secuestro de ordenadores pero esto puede resultar infructífero en muy poco tiempo por el empleo de la computación en la nube (*cloud computing*) y el almacenamiento de información en el ciberespacio o servidores en el extranjero.

La computación en la nube (*cloud computing*), será uno de los temas con los que tendrá que lidiar en los próximos años la introducción e implementación del expediente digital. En particular, con las medidas de seguridad informática y evitar almacenar información en servidores situados fuera del territorio nacional.

(2) ¿En su sistema penal se puede prescindir de la determinación del *locus delicti* en caso de cometerse un ciberdelito? ¿Por qué (no)? .

No cuando se trata de un ciberdelito en sí mismo, pero sí si se trata de un delito de jurisdicción universal cometido a través de la internet o en el cual las pruebas fundamentales están en la internet.

(3) ¿Qué normas de competencia jurisdiccional se aplican a los ciberdelitos tales como la incitación al odio a través de Internet, hacking, ataques contra los sistemas informáticos, etc? Si su Estado no tiene jurisdicción sobre estos delitos, ¿se considera es esto problemático?.

Se aplicarían las normas generales ya descriptas.

(4) ¿Su legislación nacional contiene normas relativas a la prevención o a la solución de los conflictos de jurisdicción? ¿Hay alguna práctica sobre ello?.

Si a través del principio de Territorial y Principios Extraterritoriales de extensión de la jurisdicción como Real o de Defensa, Universal o personal, pero ninguno especifico en función de Ciberdelitos.

(5) ¿En su sistema penal se puede prescindir de los principios jurisdiccionales en caso de que se cometa un ciberdelito, lo que en esencia significa que el Derecho penal nacional es de aplicación universal? ¿Debería esto limitarse a ciertos delitos, o estar condicionada a la existencia de un tratado?.

La legislación de la República Argentina no prevé en ningún supuesto la prescindencia de los principios jurisdiccionales y no ha contemplado una regulación especial para la criminalidad informática.

(C) Derecho penal sustantivo y sanciones

(1) ¿Qué ciberdelitos tipificados en su sistema penal nacional considera usted que tienen una dimensión transnacional?.

Sin dudas, el lugar el más destacado es el Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (Artículo 128 del C.P.).

A raíz de la intangibilidad del software y del almacenamiento digital de información también resultan relevantes: 1) Violación de correspondencia electrónica (Artículo 153 del C.P.), 2) Acceso ilegítimo a un sistema informático (Artículo 153 bis del C.P.), 3) Publicación abusiva de correspondencia (Artículo 155 del C.P.), 4) Revelación de secretos (Artículo 157 del C.P.), 5) Delitos relacionados con la protección de datos personales (Artículo 157 bis del C.P.), 6) Defraudación informática (artículo 173, inciso 16, C.P.), 7), Daños (artículos 183 y 184, C.P.), 8) Interrupción o entorpecimiento de las comunicaciones (artículo 197 C.P.), 9) El tipo penal de Alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (artículo 255 del C.P.),

Grupo Nacional Argentino. Contribuyeron en el presente trabajo: Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.

(2) ¿En qué medida las definiciones de los ciberdelitos contienen elementos jurisdiccionales?.

La reforma realizada por la ley 26.388 en materia de criminalidad informática no ha introducido en la descripción típica de las conductas ningún elemento que haga referencia a la jurisdicción.

(3) ¿Hasta qué punto las reglas de la parte general sobre la comisión, conspiración o cualquier otra forma de participación contienen elementos jurisdiccionales?.

La parte general de nuestro derecho penal, se aplica a todos los delitos.

(4) ¿Considera usted que los ciberdelitos constituyen un asunto que un Estado puede regular por sí mismo? Si es así, indique cómo puede hacerlo un Estado. Si no es así, indique por qué no puede hacerlo.

Puede y debe regularlo por sí mismo, pero resultará indispensable tener en cuenta la cooperación internacional y compatibilidad de la legislación. En particular por la internacionalidad que el delito informático presenta y la gran problemática que presenta la aplicación de la ley penal en el espacio.

(5) ¿Su Derecho penal nacional prevé la responsabilidad penal de las empresas / proveedores (internacionales)? ¿Tiene la atribución de responsabilidad implicaciones jurisdiccionales?.

Nuestra legislación penal no prevé la responsabilidad penal de las personas jurídicas en materia de Criminalidad Informática.

(D) Cooperación en materia penal

(1) ¿Hasta qué punto las especificidades de la tecnología de la información cambian la naturaleza de la asistencia mutua?.

No debería cambiarlas desde una perspectiva teórica. En lo práctico, las asimetrías de disponibilidad tecnológica entre los estados, pueden obstar a una efectiva asistencia mutua.

(2)(a) ¿Se prevé en su país la interceptación de telecomunicaciones (inalámbricas)? ¿Bajo qué condiciones?.

Sí, por régimen general: necesidad de orden judicial fundada.

(b) ¿En qué medida es relevante que un proveedor o un satélite puedan estar ubicados fuera de las fronteras del país?.

Resulta relevante para poder someterlo a la jurisdicción nacional.

(c) ¿Su legislación nacional prevé la asistencia judicial mutua en relación a la interceptación de las telecomunicaciones? ¿Ha celebrado su país convenios internacionales al respecto?

Desde siempre la Argentina ha participado de los tratados internacionales de cooperación en materia de adquisición y producción de pruebas. En el ámbito interno rige la Ley de Cooperación Internacional en Materia Penal (Ley 24768 de 1998), cuyos principios generales resultarían de aplicación.

(3) ¿En qué medida las causas generales de denegación se aplican en relación a las investigaciones en Internet y otros medios para acceder a los ordenadores y las redes ubicadas en otros lugares?.

En la misma que para cualquier acto de cooperación, ya que no hay previsión específica aún.

(4) ¿Se exige en su legislación nacional el requisito de la doble incriminación para la cooperación en aquellas situaciones en las que el autor haya causado los efectos desde un Estado en el que se permite la conducta en un Estado en el que se tipifica como delito la conducta?.

Si, como en los procesos de extradición.

(5) ¿Permite su legislación nacional las investigaciones extraterritoriales? ¿Bajo qué condiciones? Por favor, responda tanto a la situación en la que las autoridades

nacionales de aplicación de la ley necesitan información, como cuando las autoridades extranjeras necesitan la información disponible en su Estado.

Toda investigación en el exterior, se rige por los principios generales de la cooperación internacional, tanto si nuestros magistrados y funcionarios se constituyen en el extranjero, como si requieren esa actividad de las autoridades extranjeras. En cualquier caso, se necesita la aprobación de los magistrados del país requerido.

(6) ¿Se permite el autoservicio (*self service*) (obtención de pruebas en otro Estado sin pedir permiso)? ¿Qué condiciones deben cumplirse para permitir el autoservicio? Por favor, diferenciar la información pública y la protegida. ¿Cuál es la práctica (tanto activa como pasiva) en su país?.

No se permite. Si se trata de información privada, se rige por las reglas del derecho internacional y los principios de libertad probatoria. No existe legislación procesal penal específica sobre ese asunto en materia de cibercriminalidad.

(7) Si es así, ¿se aplica esta legislación también a las búsquedas que se llevan a cabo en la web de acceso público, o en ordenadores que se encuentran fuera del país?.

Si se puede hacer desde la Argentina, rige el principio de libertad probatoria, pero también el de defensa en juicio, que exige que la defensa haya tenido la posibilidad de controlar la prueba.

(8) ¿Es su país parte en acuerdos sobre el Registro de Nombre de Pasajero (PNR) (transacciones financieras, intercambio de ADN, cuestiones de visados o similares)? Por favor especificar y explicar cómo se lleva a cabo el intercambio de datos en la legislación nacional. ¿Tiene su país una llamada unidad que está disponible 24 horas al día y 7 días a la semana para el intercambio de datos? Limítese a las cuestiones relevantes sobre uso de la información para la investigación criminal.

Hasta la fecha no se cuenta con una unidad especializada en el intercambio de datos.

Grupo Nacional Argentino. Contribuyeron en el presente trabajo: Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.

(9) ¿Hasta qué punto los datos a que se refiere en su respuesta a la pregunta anterior se intercambian para la investigación criminal y cuál es el fundamento jurídico? ¿Hasta qué punto la persona concernida tiene la posibilidad de impedir / corregir / eliminar la información? ¿En qué medida puede esta información ser utilizada como prueba? ¿La ley de su país permite la detección y retirada de un sitio web que contiene información ilegal? ¿Existe alguna una práctica? ¿Desempeña algún papel el sitio del proveedor, propietario del sitio o cualquier otro elemento extranjero?.

La acción constitucional de hábeas data, constituye un camino de fácil y ágil acceso para el ciudadano a efectos de detectar, hacer corregir o retirar los datos personales que figuren en bases que pudieran ser no autorizados, excesivos o incorrectos.

(10) ¿Cree usted que es posible un sistema de aplicación internacional para ejecutar las decisiones (por ejemplo, órdenes de suspensión de Internet o inhabilitaciones) en el área de la delincuencia cibernética? ¿Por qué (no)?.

Sí, conforme las recomendaciones realizadas por el Convenio de Cibercriminalidad de Budapest.

(11) ¿Su país permite la consulta directa de bases de datos nacionales o internacionales que contienen información relevante para las investigaciones criminales (sin solicitud)?.

Existen registros públicos. Pero los demás no son accesibles, sino solo con orden judicial.

(12) ¿Participa su país en Interpol / Europol / Eurojust o cualquier otro organismo supranacional que aborde el intercambio de información? ¿Bajo qué condiciones?.

Si con Interpol y Europol

(E) Aspectos relacionados con los derechos humanos.

Sección 4: Documento de reflexión y cuestionario

André Klip

Grupo Nacional Argentino. Contribuyeron en el presente trabajo: Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.

(1) ¿Qué normas de derechos humanos o constitucionales son aplicables en el contexto de las investigaciones penales con tecnología de la información? ¿Es relevante para la determinación de las normas aplicables de derechos humanos dónde se considera que se han realizado las investigaciones?.

Todas en general, ninguna específica referida a la cibercriminalidad.

(2) ¿Cómo se regula la responsabilidad o rendición de cuentas (*accountability*) de su Estado involucrado en la cooperación internacional? Por ejemplo, ¿es su Estado responsable del uso de la información recolectada por otro Estado en violación de las normas internacionales de derechos humanos?.

No está regulado de manera específica.

(F) Desarrollos futuros

(1) Las modernas telecomunicaciones ofrecen la posibilidad de contactar directamente con los acusados, víctimas y testigos a través de las fronteras. ¿Se debería permitir eso y, en caso afirmativo, en qué condiciones? Si no es así, ¿se deberían aplicar las reglas clásicas de asistencia mutua (solicitud y respuesta), y por qué? .

En las audiencias de causas por graves violaciones a los Derechos Humanos y en otras de megacriminalidad, se ha permitido el uso de videoconferencia, para recibir pruebas desde el extranjero. Lo mismo ocurre con el envío de documentos escaneados, cuando son certificados en el país de origen, por ejemplo, por nuestro consulado. De modo que no sólo es aconsejable, sino que ya lo estamos haciendo.

(2) ¿Existe algún impedimento legal en su legislación para las audiencias a través de medios audiovisuales (a través de Skype o de otro medio) en casos transnacionales? Si es así ¿cuál? Si no es así, ¿hay alguna práctica?.

No existe ningún impedimento legal. No se encuentra regulado pero se usa cada vez con mayor habitualidad.

Grupo Nacional Argentino. Contribuyeron en el presente trabajo: Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.

¿Hay alguna otra cuestión relacionada con la sociedad de la información y el Derecho penal internacional que actualmente juega un papel en su país y no ha sido tratado en las preguntas anteriores?

La computación en la nube (*Cloud Computing)* y el almacenamiento de información en servidores situados fuera de la jurisdicción nacional, en particular cuando la información a resguardarse es información que pueda provenir de los organismos públicos del Estado.