*Coloquio Preparatorio*
*24 – 27 Septiembre 2013, Antalya (Turquía)*
*Sección III: Sociedad de la información y Derecho penal*

## 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. Johannes F. Nijboer por email: J.F.Nijboer@law.leidenuniv.nl

(B) Cuestiones Generales.

(1) ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del procedimiento penal (incluida la práctica forense)? ¿Cómo están reflejadas estas definiciones conceptuales en la doctrina científica, la legislación, las decisiones judiciales, y las prácticas pertinentes en el contexto del proceso penal?.

Una de las principales dificultades que presenta la Legislación Argentina en materia penal es que no se ha llevado a cabo una reforma procesal penal en materia de criminalidad informática, adaptando nuestra legislación al Convenio de Cibercriminalidad de Budapest.

Se encuentra pendiente la sanción de una ley procesal que regula la obtención, almacenamiento y conservación de prueba digital.

(2) ¿Existen instituciones específicas y / o grupos de trabajo involucrados en la aplicación de las TIC en el sistema penal?.

El Ministerio Público Fiscal tiene creada una comisión

(3) ¿Existen organizaciones (empresas) privadas (comerciales) que ofrecen servicios relacionados con las TIC en el sistema penal? Si es así, ¿puede dar ejemplos? ¿Qué límites tienen que ser observados?.

No

(C) Información e inteligencia: construyendo posiciones de información (information positions) para aplicación de la ley.

La construcción de las posiciones de información es parte de la denominada actuación policial basada en la inteligencia. Se puede definir la actuación policial basada en la inteligencia como un marco conceptual de llevar a cabo la actividad policial como un proceso de organización de la información que se permite a las agencias de aplicación de la ley en sus tareas preventivas y represivas.

* 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.

(1) ¿Qué técnicas relacionadas con las TIC se utilizan para la construcción de posiciones de información por las agencias de aplicación de la ley? .

Una de las principales que se está empleando es la geolocalización de equipos celulares, mediante la activación remota de GPS o empleo de detección de antenas utilizas por el dispositivo.

(2) ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y privadas (por ejemplo, el Registro de Nombre de Pasajero o los datos financieros como los datos de SWIFT) tienen acceso las agencias de la aplicación de la ley?.

Base de datos de la Administración Federal de Ingresos Públicos (AFIP), la Base de Datos del ANSES, de la Dirección General de Aduanas (DGA), Base de Datos de Migraciones, Base de Datos del Banco Central de la República Argentina (BCRA).

(3) ¿Pueden aplicarse las técnicas consideradas como minería de datos y comparación de datos? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? Si es así, ¿se han desarrollado herramientas especiales para las agencias de aplicación de la ley?.

No.

(4) ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la construcción de posiciones de información?.

Sí, bajo régimen general reglado en los códigos procesales: autorización judicial fundada para poder interceptar.
La interceptación de telecomunicaciones móviles se encuentra prevista.
También existe el acceso a cuentas de correo electrónico, *chat,* o mensajería instantánea móvil no sea haya implementado.
En particular, la mensajería instantánea a móvil instalada en los celulares inteligentes (*Smarthphone*) presentas serias dificultades para su posible investigación por parte de agencias judiciales y policiales debido a que este tipo de mensajería instantánea (*BlackBerry Messenger, Whatsapp*) se encuentra encriptada.

(5) ¿Qué actores privados (por ejemplo, proveedores de internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para las agencias de aplicación de la ley?.

Las empresas privadas no se encuentran obligadas por ley a la conservación de información y datos.

(6) ¿Qué actores privados pueden proporcionar o están obligados a proporcionar información a las agencias de aplicación de la ley?.

Los proveedores de internet (*Speedy, Fibertel*), los servidores de correos electrónicos (*Hotmail, Yahoo, Gmail*), los motores de búsqueda (Google, Yahoo), las Redes Sociales (*facebook, myspace, Hi5, Orkut, Sonico, Etc)*

(7) ¿Existe control judicial de la construcción de posiciones de información?.

No existen hasta la fecha organismos especializados en la construcción de información digital.

(D) Las TIC en la investigación penal.

(1) ¿Pueden las agencias de aplicación de la ley llevar a cabo intervenciones en tiempo real a) de datos sobre el tráfico , b) sobre el contenido de los datos?.

Si bien la ley 26.388 ha tenido en consideración el *"Convenio sobre la Ciberdelincuencia de Budapest"* del 23 de noviembre de 2001, es dable recordar que sólo ha seguido sus lineamientos parcialmente, más precisamente sólo ha adaptado nuestra legislación nacional en lo que refiere a Derecho penal sustantivo, previsto en el Capítulo II *"Medidas que deberán adoptarse a nivel nacional"*, Sección 1 *"Derecho penal sustantivo"*.

Por el contrario, no ha adaptado nuestra legislación a la Sección 2, destinada al *"Derecho Procesal"* por este instrumento internacional. Es así que no se adoptaron medidas legislativas que permitan establecer procedimientos penales específicos para la obtención de prueba electrónica de cualquier delito cometido por medio de un sistema informático (Art. 14 del *Convenio sobre la Ciberdelincuencia de Budapest*).

En igual sentido tampoco se ha dado cumplimiento a la sanción de una legislación que prevea la *"conservación rápida de datos informáticos almacenados"*, conforme lo requerido por el mencionado convenio en su Sección 2, Título 2.

Así es que resultaría indispensable una legislación nacional que prevea: 1) La conservación rápida de datos informáticos almacenados (Art. 16 del *Convenio sobre la Ciberdelincuencia de Budapest*); 2) Conservación y revelación parcial rápidas de los datos relativos al tráfico (Art. 17 del *Convenio sobre la Ciberdelincuencia de Budapest*); 3) Orden de presentación (Art. 18 del *Convenio sobre la Ciberdelincuencia de Budapest*); 4) Registro y confiscación de datos informáticos almacenados (Art. 19 del *Convenio sobre la Ciberdelincuencia de Budapest*); 5) Obtención en tiempo real de datos relativos al tráfico (Art. 20 del *Convenio sobre la Ciberdelincuencia de Budapest*); y 6) Interceptación de datos relativos al contenido (Art. 21 del *Convenio sobre la Ciberdelincuencia de Budapest*).

Habría que chequear con la gente de OBSERVACIONES JUDIALES (la célebre OJOTA) qué están haciendo ahora. Supongo que pueden hoy día realizar este tipo de control en tiempo real.

(2) ¿Pueden las agencias de aplicación de la ley tener acceso / congelar / investigar / secuestrar los sistemas de información sobre: a) datos sobre el tráfico, b) el contenido de los datos?

Si bien el Poder Judicial de la Nación, por medio de la Corte Suprema de Justicia de la Nación ha realizado profundas actualizaciones en materia de infraestructura tecnológica y capacitación del personal[1], lo cierto es que en la actualidad no se cuenta con ningún Juzgado Nacional especializado en materia de criminalidad informática o área destinada específicamente a esta materia.

Desgraciadamente, el Ministerio Público Fiscal (MPF), se encuentra en una situación análoga a la del Poder Judicial de la Nación, ya que si bien cuenta con un importante número de Unidades Fiscales temáticas o Unidades Especiales[2], hasta la fecha no ha creado o destinado recursos a instaurar una Unidad Fiscal especializada en criminalidad informática.

Idéntica realidad exhibe el Ministerio Público de la Defensa (MPD) quien también posee una gran cantidad de Comisiones y Programas[3], como así también un importante Departamento de Informática dentro del área de la Dirección General de Administración de la Defensoría General de la Nación, pero hasta el presente no dispone de ninguna comisión o programa especializado en criminalidad informática. En cuanto a los auxiliares de la Administración de Justicia como lo son: la Policía Federal Argentina (PFA), la Gendarmería Nacional Argentina (GNA), 3) la Prefectura Naval Argentina (PNA), 4) la Policía de Seguridad Aeroportuaria (PSA), solo los dos primeros cuentas con áreas especializadas de investigación.

(3) ¿Se puede obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley? En caso de incumplimiento, ¿hay medidas coercitivas o sanciones?. En particular resulta muy difícil realizar medidas coercitivas sobre empresas que resultan ser transnacionales como *Google, Hotmail, Yahoo, Facebook.*

(4) ¿Pueden las agencias de aplicación de la ley realizar videovigilancia? ¿Pueden obligar a las personas físicas o jurídicas a cooperar?.

La videovigilancia resulta una herramienta tecnológica permitida en espacios públicos, no así en espacio privados, ni en domicilios. No se encuentra autorizada la escucha acústica de domicilio o el empleo de cámaras térmicas.

En reforma del año 2010, se incorporó al CPPBA el Art. 265bis. Filmaciones y grabaciones (cf. Ley 14172): regula entre los medios de prueba a las filmaciones de sistemas de monitoreo público o privado y grabaciones de las llamadas a teléfonos del sistema de emergencias.

(5) ¿Pueden o deben aplicar las agencias de aplicación de la ley grabación audiovisual de los interrogatorios (sospechosos, testigos)?

Pueden realizarse grabaciones de juicios, audiencias orales antes las cámaras de apelaciones de los distintos fueros.

Hay previsiones específicas, por ejemplo, en la provincia de Buenos Aires, con relación a las declaraciones testimoniales de niñas, niños y adolescentes (art. 102 bis y cctes., cf. Ley 13954/09), que prevén el anticipo extraordinario de prueba con video-filmación u otro medio similar de registración del acto.

---

[1] Ver CORTE SUPEMA DE JUSTICIA DE LA NACIÓN. *"Justicia argentina online. La creación de la Agencia de Noticias del Poder Judicial"*, *"Argentine Justicie online. The Creation of the News Agency of the Judiciary"*.Editorial Altura Impresores, 2010.

[2] Entre sus Unidades Especiales pueden mencionarse: 1) U.F. AMIA (UFIA); 2) U.F. de Asistencia en Secuestros Extorsivos y Trata de Personas (UFASE); 3) U.F. de investigación de Delitos de Tributarios y Contrabando (UFITCO); 4) U.F. para la investigación de Delitos relativos a la Seguridad Social (UFISS); 5) U.F. para los delitos cometidos en el ámbito del PAMI (UFIPAMI); 6) U.F. para los delitos cometidos en el ámbito del Registro Nacional de Armas (UFIRENAR); 7) U.F. para la investigación de Delitos contra la Integridad Sexual y Prostitución Infantil; 8) U.F. para la investigación de delitos contra el Medio Ambiente; 9) U.F. de investigación de Lavado de Dinero y Financiamiento del Terrorismo; 10) U.F. de coordinación de causas de violación de Derechos Humanos durante el Terrorismo de Estado; 11) U.F. para la investigación de violencia en Espectáculos Deportivos; conforme http://www.mpf.gov.ar/index.asp?page=Organigrama/organigrama.html

[3] La Defensoría General de la Nación cuenta con los siguientes programas y comisiones: 1) Comisión de Cárceles; 2) Comisión de Seguimiento del Tratamiento Institucional de Niñas, Niños y Adolescentes; 3) Comisión para la Asistencia Integral y Protección al Refugiado y Peticionante de Refugio, 4) Comisión de Seguimiento del Tratamiento Institucional de Neuropsiquiátricos; 5) Comisión de Temática de Género; Comisión del Migrante; 6) Programa de Asistencia y Patrocinio Jurídico; 7) Programa para la Aplicación de Tratados Internacionales de Derechos Humanos; 8) Programa de Atención a las Problemáticas Sociales y Relaciones con la Comunidad; 9) Programa Piloto para la Asistencia Jurídica a Mujeres Privadas de la Libertad; conforme www.mpd.gov.ar

También para registrar audiencias orales en etapa de la investigación penal preparatoria y de ejecución de la pena, en que las resoluciones judiciales son oralizadas.

(E) Las TIC y la prueba.

(La cadena de etapas: recogida / almacenamiento / retención / producción / presentación / valoración de la prueba electrónica).

(1) ¿Existen reglas sobre la prueba específicas para la información relacionada con las TIC?.

Pese a existir modificaciones al Código Procesal Penal de la Nación no se ha realizado una reforma procesal penal en materia de criminalidad informática.

(2) ¿Existen reglas sobre la integridad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, hacking) de la prueba relativa a las TIC?.

Ante la ausencia de ley procesal no existen reglas de integridad o protocolos para la manipulación de prueba digital.

(3) ¿Existen reglas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas que son específicas de la información relacionada con las TIC?.

(4) ¿Existen reglas específicas sobre el descubrimiento y revelación de la prueba relacionada con las TIC?.

No debido a la carencia de una reforma procesal penal.

(5) ¿Existen reglas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?.

No debido a la carencia de una reforma procesal penal.

(F) Las TIC en la etapa de juicio

(1) Cómo puede o debe introducirse en el juicio la prueba relacionada con las TIC?.

(2) ¿Pueden realizarse interrogatorios a distancia (por ejemplo, conexiones vía satélite)?.

Se han implementado testimonial a distancia, por ejemplo en la causa AMIA, el caso del Testigo “C”.

(3) ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (asesinatos, accidentes de tráfico)?.

Sin lugar a dudas, el empleo de mapas satelitales como *Google maps* o *Google Earth,* sistemas de coordenadas, GPS y programas y aplicaciones de geolocalización como “*foursquare*”.

(4) ¿Pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido)?.

(6) ¿Pueden sustituirse los expedientes penales en "papel" por otros electrónicos? ¿Se ha avanzado hacia la digitalización de los documentos del juicio?.

Hasta la fecha no, gradualmente se producirá en la República Argentina a través de la ley 26.685, la transición al expediente digital y la gradual sustitución del expediente en soporte papel.

Un significativo avance pro parte del Poder Judicial de la Nación de la República Argentina, es la labor encarad por la Corte Suprema de Justicia de la Nación, quien ha digitalizado todas sus sentencias y gran parte de su biblioteca. En igual sentido ha comenzado con los cursos de capacitación para la implementación gradual de la acordada 31/2011 tendiente a la constitución de domicilios electrónicos de notificación.

No debe perderse de vista que, en un país con estructura federal en el que los códigos procesales han quedado reservados a las provincias y, además, el Código Procesal Penal de la Nación es de los más antiguos en cuanto a su adscripción a un sistema mixto con rasgos inquisitivos, en el orden local puede haber previsiones más actuales, como las citadas de la provincia de Buenos Aires, donde hoy es común que actos centrales del proceso se documenten mediante registración de audio/video digitales con una breve acta escrita que complementa en el legajo tradicional, dejándose constancia del acto celebrado.