"PAUTAS INFORMATIVAS Y PROCEDIMENTALES EN CYBERDELITOS" (Experiencia de la Ciudad de Córdoba)

José Francisco Arce, Juan Pablo Galli Funes y Diego Gabriel Zabala
Miembros del Poder Judicial de Córdoba – Ministerio Público Fiscal –
Policía Judicial –Sección Informática Forense.
jarce@justiciacordoba.gov.ar

Abstract. A 3 años de la sanción de la ley de delitos informáticos, empiezan a pasar a un segundo plano las cuestiones teóricas y cobran relevancia las experiencias prácticas en cuestiones procedimentales y de investigación en esta materia. La inter-disciplina, como en toda la ciencia Penal, cobra importancia a la hora del descubrimiento de la verdad real. Esto sumado a las nuevas características de la sociedad de la información y en especial el manejo de la información que circula por Internet; las dificultades de los trabajos de campo e investigación por las características de los elementos o información a recolectar o buscar y la corta experiencia de nuestros tribunales hacen necesarias las investigaciones y la difusión de las diversas experiencias de los órganos técnicos avocados a la investigación de los de delitos con la intervención de las TICs.

Keywords: Delitos–TICs–Inter-disciplina–Experiencias Practicas - Necesidades

1. Introducción

La "cyber-seguridad" se ha convertido en los últimos tiempos en un término muy utilizado por los distintos países a la hora de dar respuesta a las nuevas demandas de la sociedad. Y pronto se convirtió en parte integrante de nuevos servicios y de la política Gubernamental. Según la I.T.U [1]. a nivel nacional se trata de una responsabilidad compartida que requerirá de acciones coordinadas para la prevención, preparación y respuesta de la normalidad, y a nivel internacional o regional la cooperación y colaboración con los socios.

A nivel mundial se han desarrollado ya hace tiempo avances significativos en materia de cooperación y colaboración, iniciativas de organizaciones gubernamentales como no gubernamentales, tales como el convenio del ciber-delito de Budapest, elaborado

[1] Unión Internacional de Telecomunicaciones. EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO. División de Aplicaciones TIC y Ciberseguridad, Departamento de Políticas y Estrategias, Sector de Desarrollo de las Telecomunicaciones de la UIT. Proyecto de abril de 2009

por el Consejo de Europa en el año 2001 y del cual Argentina solicito su adhesión siendo admitida y ratificada a partir de este año.

Desde hace un tiempo muchos países, incluido el nuestro, han visto la necesidad de enfrentar este tipo de ilícitos, tratar de legislar normas de fondo específica de la materia y adaptar las de forma, como así también crear grupos técnicos especiales en la materia.

Lo cierto es que cada país tiene dado un marco normativo de fondo (que dicen los derechos) y de forma (que reglamentan las formas) que se fue adaptando a lo largo del tiempo lo más que pudo a la realidad mutante de las sociedades todas, al igual que la capacitación permanente de los distintos operadores jurídicos fue siempre más por detrás de los cambios.

Dentro de la administración de Justicia nos encontramos con una manera ya institucionalizada procedimental en la investigación de delitos convencionales. A medida que fue pasando el tiempo algunos delitos con nuevas modalidades empezaron a ser vistos desde otra óptica y con la necesidad de una forma especial de tratamiento e investigación, que llevo a la especialidad por ejemplo en diversos ámbitos como el académico y hasta el judicial, como paso con el fuero "Penal Económico" aquí en Córdoba. Considerando que las modalidades y los medios utilizados en materia de delitos informáticos ameritan un tratamiento especial a la hora abordar las investigaciones pertinentes. Y ante esta necesidad es menester que en la actualidad los distintos procedimientos se agiornen para dar respuesta a estas situaciones, que carecen de una guía teórica-procedimental que agilice el trámite y la investigación de este tipo de delitos.

1.1. Fundamentación:

A partir de la sanción de la ley 26.388 que significo la incorporación de una serie de delitos informáticos al Código Penal se comenzó a recorrer un camino nuevo lleno de desafíos. Antes de la sanción de la ley misma solo había normas parciales con soluciones insuficientes.

Sin la ley muchos casos no pudieron tener los resultados esperados a pesar de dar con los responsables de los hechos. Bien lo aclara Pablo Palazzi en su libro [2] que los jueces penales que se enfrentan a estos casos muchas veces se ven obligados a declarar acciones atípicas que son claramente perjudiciales. Y otros casos no tuvieron éxito por las características de las investigaciones y los medios utilizados en la comisión de los daños, ya que la prueba informática o digital, requiere para su

[2] Pablo Palazzi. "Los Delitos Informáticos en el Código Penal". Abeledo Perrot. Mayo de 2009.

obtención y conservación otro tipo de abordaje de los utilizados hasta ese momento que impidieron se haga justicia y se evite la impunidad.

1.2 Características Particulares para el marco de trabajo.

1- Se debe realizar una investigación minuciosa preliminar y una planificación con el tiempo necesario por parte del operador judicial para determinar la ubicación y características técnicas generales de los elementos a secuestrar por medio de la policía[3].

2- Se trata de una actividad Multidisciplinaria que deberá ser tenida en cuenta dada la necesidad de interactuar con profesionales de otras áreas.

3- Internacionalización de los delitos. Cooperación Internacional es una de las claves a la hora de tener éxito en las investigaciones.

4- Volatibilidad de la prueba. Se tendrá que considerar la capacitación previa o el pronto pedido de instrucciones a personal capacitado.

5- Nuevo escenario. Llamado "La Nube" (Cyber-Espacio) – Falta de Territorialidad definida.

6- Avances explosivos en el campo de la TICs.

2. Trabajo de Campo

Bajo este título pretendemos brindar a los lectores y operadores de la justicia en general "*pautas generales de procedimiento"* una vez ordenado el mismo; hablamos de procedimientos destinados a la investigación de delitos informáticos. No pretendemos agotar todas las situaciones fácticas posibles, sino que ante la realidad de las características de los delitos, sumada la difícil situación a la que se enfrentan sus operadores con la prueba, solo brindar una especie de guía práctica para el desarrollo del mismo.

Creemos que estas pautas operativas en el abordaje inicial a un lugar relacionado con un supuesto delito, con la incertidumbre de no saber con qué nos encontraremos, son fundamentales a la hora de asegurarnos la obtención y preservación de la evidencia digital o informática.

Es en esta tarea que creemos relevante tener en cuenta las siguientes situaciones [4]:

[3] Policía Administrativa y Judicial.

[4] Para la elaboración del presente se tuvo en cuenta no solo, la larga experiencia de los departamentos técnicos de la Provincia de Córdoba, sino también de trabajos realizados por otras provincias, como es el caso del Lic y Abog. Sebastián Gómez de la provincia de Neuquén,

1- Con relación a las personas: - separar aquellas que estén trabajando sobre los equipos informáticos y/o telefonía móvil y no permitirles volver a utilizarlos.

2- En caso de tratarse de una empresa, proceder a la identificación del personal informático interno y externo.

3- Fotografiar la escena del crimen tal cual como se presenta, con relación a los elementos. Toma completa del sitio donde están los equipos, pantallas de los equipos si se encuentran encendidas, en su caso, filmar.

4- Evitar tocar elementos informáticos del delitos sin guantes descartables, ya sea pantallas, teclados, mouse.

5- En caso de estar apagados, dejarlos así; si están encendidos, consultar con un experto. Si no se reconoce su estado tratarlos como si estuvieran prendido.

6- Identificar Usuarios de aplicaciones especificas por puestos (ej: programadores dentro de la empresa y usuarios)

7- Registrar nombre del equipo informático, fecha hora, configuración regional, operador activo y nomina de usuarios del equipo.

8- En lo posible obtener contraseñas de aplicaciones y sistemas operativos e incorporarlas en el acta

9- Tratar de establecer si las computadoras trabajan en Red entre sí, procurar identificar redes fuera de la organización o domicilio y ante la duda, consultar y esperar los consejos de un experto.

10- Si no sabe como apagar y no hay un experto para asesorarlo desconectar la energía desde el cable conectado en el gabinete, si son notebooks quitar la o las baterías y secuestrar cables y fuentes de alimentación, anotar la fecha, la hora y las acciones realizadas

11- Preferiblemente secuestrar solo los dispositivos de almacenamiento de información (disco rígido, pen drive, stick de memoria, memoria para celulares, etc.), sin efectuar análisis de contenido para evitar su desnaturalización. Consultar con el Técnico

12- Respecto de DVD, CD, etc. Analizar contenido para evitar secuestros innecesarios, dependiendo la situación. En todos los casos de secuestro de material “trucho”, en el acta usar la expresión “aparentemente apócrifo”. Consultar al técnico.

13- Identificar todos los elementos motivo de secuestro. Ante la situación de encontrarse con elementos de apariencia semejante (computadoras parecidas)

---

y trabajo de organismos diversos países, como del FBI de Estados Unidos en materia de informática forense.

otorgarle identificación secuencial con números o letras. Ej: Números o Letras. Cuando no se sepa con claridad en presencia de que dispositivo se encuentra describirlo de la forma más detallada posible en cuanto a sus señas particulares (no se distingue si es un CD o DVD o dispositivo electrónico especifico).

14- En caso de grandes volúmenes de CD y/o DVD los cuales son contenidos en diversos recipientes (torres, cajas) se debe identificar la cantidad que hay en cada uno de los contenedores como la identificación del mismo de acuerdo a la metodología del párrafo anterior.

15- Preservar - procurar utilizar envoltorio de cartón y o papel para la preservación de los elementos a secuestrar evitando elementos de envoltorio de nylon o polietileno. Precintar la toma de energía para prevenir riesgos.

16- La autoridad judicial (FISCAL) designa el destino y responsables de los elementos a secuestrar.

17- El recinto donde se alojen los elementos secuestrados debe estar limpio y en resguardo de altas temperaturas.

18- Al momento de la recepción del material a analizar se debe hacer constar condiciones (medio de envoltorio o preservación, faja de garantía y elementos tendientes a su individualización), fotografiar para acreditar dichas condiciones. Emitiendo recibo correspondiente.

2.1. Problemáticas:

Analizando las diversas problemáticas surgidas en el lugar del hecho, basada en la experiencia de "Policía Judicial de la Provincia de Córdoba [5]", pudimos relevar diversas cuestiones que permitirán maximizar las condiciones de investigación y minimizar los errores y dificultades propias de este tipo de abordaje.

Trataremos de realizar un breve resumen de las problemáticas más comunes de los trabajos de campo, seguidas de propuestas superadoras de las situaciones para ser tenidas en cuenta por todos los actores involucrados. Por ese motivo lo que se pretende es tener una mirada integral de la situación.

a.- Condiciones hostiles o desfavorables

No solo hacemos referencia a las condiciones climáticas que pueden ser un verdadero dolor de cabeza, por ejemplo si llegando al lugar del hecho nos encontramos con un lugar sin energía eléctrica o cortes sucesivos a causa del clima; sino también hablamos de estar en el lugar del supuesto hecho y no poder ingresar a alguna CPU,

[5] www.mpfcordoba.gov.ar

sistema o base de datos por no encontrase el administrador de sistemas, para obtener permisos y accesos suficientes a los mismos.

Propuesta Superadora: Tratar de identificar de antemano si el lugar donde concurrimos posee una persona encargada de los sistemas de información y procurar que se encuentre o saber dónde encontrarla.

b.- Escasas precisiones

La realidad muestra que las solicitudes de cooperación de las áreas Judiciales a las técnicas, y en particular la "Informática Forense" se realizan horas antes del abordaje o con un día de anticipación, sin brindar más datos que el pedido. Por lo que "No se conoce la causa, lugar a abordar, ni elementos a buscar".

Esta falta de información se traduce en dificultades a la hora de tomar dediciones, por ejemplo de que elementos llevar al lugar, a causa de no poder proyectar con que posible escenario nos encontraremos (Domicilio particular, empresas, organismos públicos) y ni siquiera elementos o información a buscar.

Propuesta Superadora: Se pretende que los órganos que soliciten colaboración del órgano técnico tengan en cuenta las siguientes cuestiones:

1.- Solicitar tratando de utilizar, en el caso de que corresponda, las palabras ***"...IMPRESION Y/O RESGUARDO DE ..."*** para prever la posibilidad de encontrar impedimento de efectuar alguna de las dos cosas.

2. Solicitar tratando de utilizar, en el caso de que corresponda, las palabras ***"...RESGUARDO (BACKUP) DE ..."*** cuando se prevee traer solamente determinados archivos

Como también es importante aportar ciertos datos de la causa, tal como se los describe en los puntos siguientes.

c.- Instrumental Técnico Insuficiente

Muchas veces ha ocurrido encontrase en trabajo de campo y los materiales o herramientas llevadas para el desarrollo del mismo resulta insuficiente, por ejemplo como se explico en el punto anterior, a causa de escasas precisiones e información o falta de previsibilidad. Ej.: En una causa de pedofilia, entre el instrumental llevado al procedimiento se omitió colocar un lector universal de tarjetas.

Propuesta Superadora: Aportar ciertos datos de la causa. Que se traducirá en la gestión de dos actores fundamentalmente. El judicial propiamente dicho que deberá remitir oficio con información que ayude a la investigación, y en el caso de que no lo

haga, el área técnica deberá procurar comunicación, cualquier vía, con el órgano Judicial y solicitar información que procure necesaria.

d.- El tiempo como factor delicado.

El trabajo que se realiza de campo ya sea por "relevamiento" como por "allanamiento" es finito, eso significa que debe existir un inicio y una finalización determinado, por lo que el factor tiempo juega un rol fundamental a la hora de realizar tareas en vivo [6], ya que pueden presentarse situaciones en las que se deba resguardar evidencia para posteriormente ser analizada en el laboratorio y ese resguardo o adquisición, por el volumen de la información, se hace imposible.

Otra situación en donde el tiempo es enemigo, se da cuando al lugar del hecho no concurren, en un primer momento, personal técnico idóneo y tenemos la situación de computadoras conectadas con otras o con servidores que están en otro lugar físico alejado (desconocido) y hay riesgo de que si no se resguarda pronto, sea desconectada localmente o remotamente [7].

Propuesta Superadora: Aportar datos de la causa, más vocablos de búsqueda no comunes. Lo que permitirá realizar búsquedas más directas y rápidas en el caso de que no se pueda secuestrar los equipamientos por cualquier motivo [8] o el tiempo sea limitado por la posibilidad de que se pierda la información. O en caso contrario permitir la posibilidad de secuestro de computadoras ante la imposibilidad de efectuar resguardo.

e.- No se considera la Interdisciplina.

Hace referencia a una realidad que pocos funcionarios tienen en cuenta a la hora de solicitar una colaboración a los órganos técnicos en general. En la actuación diaria, de los órganos técnicos en general, tienen que concurrir a diversos lugares que desarrollan tareas profesionales especificas, de las cuales se desconocen esa tipo de ciencia, la forma de actuar, trabajar y llevar adelante sus tareas, que serian de utilidad conocerlas a los fines de saber "***cómo y dónde***" hacer el abordaje investigativo y operativo.

EJ.: En una causa de mala praxis, en una oportunidad se allana la clínica, y la Fiscalía considerando insuficientes los elementos obtenidos, ordena un nuevo allanamiento. En la segunda oportunidad con la colaboración de un médico legista. El Dr. busco un libro que se lleva en quirófano, en el cual estaban los integrantes del nosocomio que participaron en la operación.

---

[6] Se entiende por tareas en vivo las realizadas en el lugar del hecho, en contraposición de las que se realizan en el laboratorio forense.

[7] Remotamente hace referencia a que puede ser accedida desde otro dispositivo, sin importar la distancia, mientras esté conectado a internet.

[8] En el caso de que sean necesarios para el normal funcionamiento de la empresa.

La interdisciplina se constituye hoy en día como una modalidad de actuación de la cual no podemos prescindir, por el hecho de muchos hechos a investigar tienen una complejidad de la cual es imposible abordar con una mirada unidimensional.

Propuesta Superadora: Permitir la posibilidad de secuestro de computadoras ante la imposibilidad de efectuar resguardo. Esto nos dará la posibilidad de trabajar en el laboratorio y solicitar la colaboración de otra área técnica.

f.- Planificación de la labor Forense. La planificación es algo que pertenece al mundo de la logística [9]. En este caso en particular hacemos referencia a todas las previsiones que tenemos que tener en cuenta a la hora de haberse recibido un pedido de colaboración para asistir a un lugar determinado. Estas cuestiones se traducen en distancia hasta el lugar, fecha de concurrencia, especificaciones del lugar donde se concurren, tipo de hecho que se investiga, actuaciones de otras aéreas técnicas, condiciones generales de cualquier abordaje. A modo de ejemplo:

Ej1.: En un hecho donde una filmación registrada en un equipamiento que estaba en una garita fronteriza de la provincia de Córdoba con San Luis, donde se pone en conocimiento que en 48 horas la filiación se sobre escribe. La falta de coordinación para armar un equipo interdisciplinario hizo llegar tarde para recolectar la filmación.

Ej2.: Agosto de año 2008 piquetes en la ruta por problemática del campo y falta de combustible. Había pactada una pericia con peritos de parte en la ciudad de Rio IV, se debió salir 02 horas antes para poder evitar los cortes de ruta y tener el tanque con combustible lleno, por lo que la carga se debió hacer dos días anteriores a la partida.

Propuesta Superadora: Aportar datos de la causa: Ej. En una causa de amenazas, al conseguir que la Fiscalía interviniente pasara previo al allanamiento fax de la esquela impresa. Permitió establecer la fuente utilizada y armar un archivo con contenido idéntico y estructura semejante. Eso permitió buscar la fuente en el allanamiento (encontrada en 3 de las 4 pcs) y obtener con el archivo confeccionado impresiones testigo para aportar a grafo crítica.

3 Trabajo de Laboratorio

El mismo consta de todas las tareas que se realizan en el lugar o asiento físico del área técnica tendientes a la obtención de evidencia, digital en este caso, independientemente del medio en el que se aporte, que pueda servir como prueba en un proceso judicial, para fundar una acusación y llegar a un juicio, para la posterior condena.

[9] Conjunto de medios y métodos necesarios para llevar a cabo la organización de una empresa, o de un servicio.

Como toda técnica forense, se trata, en la medida de lo posible, de conservar el estado original del objeto en estudio, por lo que se utilizan métodos para la extracción de la evidencia sin la desnaturalización del mismo, entre los que encontramos la adquisición de la imagen forense bit a bit del dispositivo de almacenamiento en estudio como Pendrive, Tarjeta de Memoria, PC, Notebook, etc.

Al igual que pasa en el trabajo de campo muchas veces no se conoce la causa, ni los elementos a buscar. Esto pasa también cuando llegan oficios directos para hacer tareas de laboratorio, donde solo se tiene para trabajar, una dirección de correo electrónica, el nombre del denunciante y nada más, lo cual conlleva a resaltar la necesidad de llevarles a los actores involucrados determinadas formas de solicitar información que se adecuan a las tareas del área técnica específica. Por ejemplo;

a.- Obtener propiedades del correo electrónico para establecer el origen de un correo electrónico.

b.- Obtener resguardo de carpetas o bases de datos con contenidos de la cuenta de correo aaa@mail.com.

c.- Aportar cotas o límites de fechas.

d.- Aportar cotas o límites de elementos.

e.- Ilustrar ciertos datos de la causa (Imágenes y/o videos de determinado índole) y forma.

f.- Aportar vocablos **no comunes** para su búsqueda.

Otro punto es el avance tecnológico, que hace que los instrumentales técnicos queden obsoletos con el corto paso del tiempo. Se debe tratar de contar con herramientas que cubran la mayor parte del espectro de casos conocidos y posibles, como así también la constante capacitación del personal técnico. Lo que no nos exime de tener que comprar instrumental específico para una causa en particular en situaciones extraordinarias.

En este punto entra en juego la planificación que depende de un presupuesto asignado, que el área tuvo y tiene en cuanto al equipamiento del laboratorio forense informático. Contar con personal que entiende y conoce la causa presente en las tareas de análisis de evidencia, ayuda a la planificación.

Otra instancia a tener en cuenta es la Antiforensia que se manifiesta ante cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa en la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense. Son técnicas que permiten borrar las huellas que puedan

haber quedado o para ocultar o enmascarar la evidencia que entorpece la tarea de los investigadores.

Ej: Uso de criptografía [10] para volúmenes de almacenamiento, Esteganografía [11] para ocultar datos; Auto-troceado de ficheros; Borrado seguro.

4.- Consideraciones a tener en cuenta a la hora de oficiar a las empresas. Formalidades e información a solicitar.

Importante tarea para complementar el trabajo de campo y laboratorio es brindar a los distintos operadores información útil para tratar con distintas empresas vinculadas a la esfera de las nuevas tecnologías, es decir, consideraciones a tener en cuenta, y formalismos que exigen algunas de ellas para brindar información.
Cabe aclarar que muchas de las empresas donde se solicitara información no tienen oficinas en nuestro país, por lo que hay que ajustarse a los procedimientos previstas por ellos y esperar que envíen la información de buena fe, ya que no existe obligación de las mismas a responder a una solicitud Judicial, salvo exhorto Internacional [12].
Las empresas con asiento en la Republica Argentina, ejemplo concreto el de los proveedores de Servicio de Internet (ISP) , en la actualidad no tienen la obligación normativa-legal de guardar información de los servicios que prestan, si se le suma el alto costo que incurren si debieran hacerlo, nos lleva a que la información que debemos solicitar tiene que tramitarse por una vía idónea y rápida, con la ayuda de todos los operadores jurídicos sin trabas procesales que impidan que esa información se diluya con el tiempo.
Es en esta nueva forma de comunicarse de las personas, como los mails, redes sociales, los espacios comunes para compartir fotos etc, es donde encontramos la necesidad de que aquellas empresas nos suministren la información relevante para las investigaciones de nuevas modalidades delictivas.

4.1. A tener en cuenta:

a.- Contenidos:

[10] Es la técnica (bien sea aplicada al arte o la ciencia) que altera las representaciones Lingüísticas de un mensaje (Wikipedia).
[11] Es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido. Si bien la esteganografía suele confundirse con la criptografía, por ser ambas parte de los procesos de protección de la información, son disciplinas bastante distintas, tanto en su forma de implementar como en su objetivo mismo. Mientras que la criptografía se utiliza para cifrar o codificar información de manera que sea ininteligible para un probable intruso (wikipedia).
[12] El trámite de exhorto tarda alrededor de un año en tramitarse. Tiempo que no se ajusta con los de una investigación criminal ordinaria.

En cuanto al contenido de los oficios, es decir, la información a solicitar a las empresas, hay que tener cuidado, ante cualquier duda consultar siempre con un técnico especializado, ya que muchas veces el vocabulario técnico puede llevarnos a cometer alguna equivocación y por ende un mal pedido a las empresas.
Hay que asegurarse que el instructor de la causa tenga una capacitación básica en cuestiones de nuevas tecnologías de la información y comunicación, de no tenerla se deberá solicitar cooperación o colaboración a los órganos técnicos de apoyo.-
Nos toparemos con diversos servicios en la web de los cuales deberemos tener conocimiento de que empresas son lo que los administran y para que se utilizan los mismos. Es decir Identificar con anticipación los diversos servicios [13] de las empresas en la web.

b.- Información Actualizada:
Tener en cuenta que las direcciones postales, de correo electrónico y los teléfonos de las empresas pueden cambiar con el tiempo. Verificar siempre con alguno de estos datos antes de enviar las solicitudes de información.
Lo aconsejable es tratar de tener una comunicación telefónica previa para corroborar no solamente los datos postales de la sede de la empresa, sino también para verificar si tiene alguna formalidad nueva, si no la tenía, para el pedido de la misma.

c.- Forma:
Tener presente que algunas empresas desarrollan modelos estándar para el pedido de la información. Es decir ellas se organizan, ante la cantidad de pedidos, de una manera que elaboran preformas. Es importante cumplirlas ya que de esta manera se está ayudando a las mismas a que puedan cumplir con la amplia demanda de pedidos que tienen.

d.- Tiempos:
La mayoría de las empresas tiene una demora importante para enviar sus respuestas. El tiempo promedio es de dos semanas, pero gran parte de ellas tienen mecanismos más rápidos en casos de máxima urgencia, con la posibilidad de enviarla la respuesta por correo electrónico, previo envío de un fax con el oficio judicial correspondiente. Es conveniente consultar con los responsables las vías extraordinarias en casos especiales, como los de desaparición de personas, secuestros o pedofilia.
Así mismo las mismas ante un pedido formal de parte de la justicia guardan la información por un periodo de 90 días que se puede extender, dependiendo la empresa, por dos términos iguales.

e.- Convenios:

[13]Ej: Microsoft ofrece diversos servicios : “Windows Live”, “Windows Lives ID (Passport)”, Windows Lives Spaces, “MSN”, “MSN Groups”, “Windows Live SkyDrive Service” y “Office Live Service”.Tambien a medida que pasa el tiempo las empresas brindan nuevos productos y servicios como es el caso de las consolas de video juego denominadas “X box”. Ellas son usadas en la actualidad como medio e instrumento para cometer delitos a través de Internet, ya que las consolas pueden funcionar On-Line. En este caso debemos solicitar a la empresa los datos pertinentes del caso.

La importancia de tratar de cerrar convenios con las empresas privadas para colaboración y cooperación mutua se vuelven de gran importancia. Por ejemplo: El Ministerio Publico Fiscal de la Provincia de Córdoba con fecha 09 de abril del año 2010, firmo un convenio con la empresa "Microsoft" que otorga alta prioridad a la modernización tecnológica y a la capacitación de los fiscales en la investigación de los delitos informáticos. En virtud de ello, expresó su satisfacción porque "la firma de este convenio es un paso más para alcanzar un Protocolo de Actuación para fiscales e investigadores en delitos informáticos o cyber crime" [14].

5. Comunicaciones con Tribunales extranjeros y Normativa

Solo de manera enunciativa veremos la normativa existente a nivel local, Nacional, regional y mundial, como así diferentes iniciativas que están regulando actualmente y otras que intentan regular o la problemática de las nuevas tecnologías y en especial en materia de Cibercrimen. Asi mismo normativa de procedimientos existentes en relación a las comunicaciones y cooperaciones internacionales en materia judicial, específicamente en materia penal. Es decir, en el caso de encontrarnos con un delito de naturaleza informático que involucre la participación de otro país, a través de que instrumentos legales solicitar cooperación y colaboración para la investigación y recolección de evidencia.

5.1.- Legislación en materia procesal.

a.- Provincia de Córdoba: Código Procesal Penal

El citado código hace referencia a los procedimientos que deben seguirse en la provincia de Córdoba en todo trámite judicial del fuero penal. Trámites que deben cumplir los órganos de administración como los administrados. El capitulo V del Código Procesal Penal Provincial, en los art 160[15] y 161[16] regula las comunicaciones entre magistrados y funcionarios provinciales con otros jueces o fiscales de diversa jurisdicción dentro del país-provincias, o federales, o bien con aquellos que se desempeñan en un Estado Extranjero.

b.- Legislación Nacional e Internacional.

La ley nacional 24.767:

[14]http://www.mpfcordoba.gov.ar/noticias_ver.aspx?id=1041

[15] Los exhortos a Tribunales extranjeros- art. 160 CPP- serán diligenciados " *mediante el Tribunal Superior de por vía diplomática en la forma prescripta por los tratados o costumbres internacionales"*

[16] art. 161 del CPP agrega " *serán diligenciados en los casos y formas establecidas por los tratados o costumbres internacionales y por las* ***leyes*** *del país cuando lo disponga el Tribunal Superior"*

De "COOPERACION INTERNACIONAL EN MATERIA PENAL", sancionada el 18 de diciembre de 1996 y promulgada de hecho el 13 de enero de 1997 en sus disposiciones generales afirma que "*Argentina prestará a cualquier Estado que lo requiera la más amplia ayuda relacionada con la investigación, el juzgamiento y la punición de delitos que correspondan a la jurisdicción de aquel.*

Normativa Internacional:

Convención de Budapest: En materia de cyberdelitos en marzo de este año la Argentina ha adherido a la Convención de Budapest del 2001[17], primera convención internacional sobre el tema, que fuera redactada por el Consejo de Europa junto a Estados Unidos, Canadá Japón, Costa Rica , México y Sudáfrica. De los 47 países adherentes solo 30 de ellos ratificaron la misma.[18] Esta decisión de Argentina se enmarca en las políticas que el país viene llevando adelante en materia internacional.

Esta convención brinda un marco veloz y seguro de cooperación y colaboración internacional para la persecución de estos delitos, mediante la cooperación de fuerzas de los distintos países y el asesoramiento de expertos técnicos. Así lo sostuvo el Subsecretario de Tecnologías de Gestión Eduardo Thill [19] quién encabezó la delegación argentina que participó de la 5ta. Conferencia anual sobre cyberdelito del Consejo de Europa

c. Principales iniciativas Mundiales

El presente pretende dar cuenta de las vastas iniciativas que se encuentran a nivel mundial que tienen de forma directa (Delitos Informáticos) o indirecta (Seguridad de la Información) a prevenir y solucionar los grandes perjuicios que esta ocasionando el mal uso de las Tics. Se aborda una visión regional y mundial que tiende a dar cuenta de la preocupación mundial en materia de Delitos y a incentivar a la investigación por

[17] Con la salvedad de que aun no se ha dado el proceso de ratificación.

[18] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/11/2010&CL=ENG

[19] En su exposición afirmó "*el crimen ha avanzado acorde a las nuevas tecnologías con lo cual no reconoce fronteras y todo el esfuerzo en capitalizar y generar mejores herramientas en nuestras agencias federales, hoy en dia no tendrían mayor sentido si no hay una integración regional y una integración internacional para la lucha en esta materia… en nuestro país nos sentimos abocados a incorporarnos a distintos planos internacionales que luchan contra el ciberdelito. Por eso en muy importante que hoy estemos aquí para expresar formalmente la fuerte convicción de nuestro país en las acciones internaciones que tengn que ver con la lucha contra el ciberdelito". Publicado por EARENDIL ON 31 marzo 2010.*

los grandes desafíos[20] que estas iniciativas y la realidad de la sociedad de la información provocan en nuestros tiempos.

a.- Organización de Naciones Unidas:
Resoluciones:

- Resoluciones de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la "lucha contra la utilización de la tecnología de la información con fines delictivos".

CNUDMI: Grupo trabajo:

- Ley Modelo sobre comercio electrónico 1996
- Ley modelos sobre firmas electrónicas 2001
- Convención sobre contrataciones electrónicas 2005

OCDE:

- Directrices de la OCDE para la Seguridad de los sistemas Informáticos y de las Redes. Hacia una cultura de la Ciberseguridad.

b.- Cumbre Mundial de la Sociedad de la Información:

- En la cumbre del año 2005, realizada en Tunez, se hicieron declaraciones[21] acerca de la problemática de la seguridad informática, haciendo hincapié en la lucha contra el delito y el convenio de Budapest del año 2001.
- El Plan de Acción de la Sociedad de la Información en América Latina y el Caribe, *eLAC*[22] *2007 y* el Plan *eLAC 2010*, han abordado el tema de la Ciberseguridad en la región como un tema prioritario

c.- Unión Europea:

[20] Algunos Desafíos son: Cooperación y coordinación internacional, Armonización Internacional de la Legislación, Capacitación Continua de los profesionales, Difusión (Outreach), Alfabetización Digital.

[21] "39. Pretendemos crear confianza de los usuarios y seguridad en la utilización de las TIC fortaleciendo el marco de confianza. Reafirmamos la necesidad de continuar promoviendo, desarrollando e implementando en colaboración con todas las partes interesadas una cultura mundial de ciberseguridad, como se indica en la Resolución 57/239 de la Asamblea General de las Naciones Unidas y en otros marcos regionales relevantes. Esta cultura requiere acción nacional y un incremento de la cooperación internacional para fortalecer la seguridad mejorando al mismo tiempo la protección de la información, privacidad y datos personales. El desarrollo continuo de la cultura de ciberseguridad debería mejorar el acceso y el comercio y debe tener en cuenta el nivel de desarrollo social y económico de cada país y respetar los aspectos orientados al desarrollo de la Sociedad de la Información." "40. Destacamos la importancia de enjuiciar la ciberdelincuencia, incluida la que se produce en una jurisdicción pero repercute en otra. Destacamos además la necesidad de concebir instrumentos y mecanismos nacionales e internacionales eficaces y eficientes, para promover la cooperación internacional, entre otros, de los organismos encargados de aplicar la ley en materia de ciberdelincuencia. Instamos a los gobiernos a que, en cooperación con otras partes interesadas, promulguen leyes que hagan posible la investigación y enjuiciamiento de la ciberdelincuencia, respetando los marcos vigentes, por ejemplo, las Resoluciones de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la lucha contra la utilización de la tecnología de la información con fines delictivos y el Convenio sobre el Delito Cibernético del Consejo de Europa."

[22] www.eclac.org/socinfo/elac/

- Directivas sobre firmas electrónicas, comercio electrónico y facturación electrónica
- Directiva 2006/24/CE del Parlamento y Consejo Europeo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicación.

d.- Unión Internacional de Telecomunicaciones[23]:

- En virtud de la línea "C5. Creación de confianza y seguridad en la utilización de las TIC" del Plan de Acción hacia la Segunda Fase de la CMSI en Túnez (2005), la UIT desarrolló la "Agenda sobre Ciberseguridad Global34" sobre los siguientes cinco ejes temáticos: i) medidas legales; ii) medidas técnicas y de procedimiento; iii) estructuras institucionales; iv) creación de capacidades, y v) cooperación internacional.
- El "Programa sobre Ciberseguridad para apoyar a los Países en Desarrollo para 2007 a 200935"[24].

e.- Otros actores con iniciativas a nivel de seguridad de la información que deben tenerse en cuenta a los fines de ver de forma integral los delitos informaticos:

- ASPAN (Asociación para la seguridad y la prosperidad en América del Norte).
- APEC[25] (Foro de cooperación Asia-Pacifico)
- BANCO MUNDIAL[26]

6. Conclusiones

Vimos en un primer momento los fundamentos teóricos que sustentan la necesidad de avanzar con las investigaciones en cibercrimen y la importancia de tratar de difundir las diversas experiencias para que podamos todos estar lo más actualizados a la hora de la investigación. Luego analizamos las tareas de campo y de laboratorio, de la parte técnica específicamente, para poder llevarles las necesidades que requieren los distintos escenarios posibles para ser proactivos y evitar situaciones que entorpezcan la obtención de evidencia. Complementada esta mirada con la normativa existente, las iniciativas mundiales, sumando los consejos útiles para tratar con diversas empresas que son las poseedoras de información relevante, creemos que todo esto es una mirada integral, para esta clase de delitos, que debe ser tenida en cuenta por todos los operarios de la Justicia, sin importar los estratos, a los fines de una mejor administración de Justicia.

[23] http://www.itu.int/es/Pages/default.aspx

[24] Aborda, entre otros temas: i) la administración general y la coordinación de los temas de ciberseguridad; ii) los requerimientos y capacidades para la asistencia mutua en temas de ciberseguridad de los Estados Miembros de la UIT; iii) las estrategias nacionales; iv) la legislación y los mecanismos de ejecución de las leyes; v) las capacidades para la observación, prevención y respuesta de incidentes; vi) el combate al Spam y las amenazas relacionadas; vii) el proyecto para mejorar la ciberseguridad y combatir el Spam; viii) las medidas para cubrir la brecha en materia de estándares de ciberseguridad; ix) los indicadores de ciberseguridad para fortalecer las actividades de cooperación regional; x) el intercambio de información y el apoyo a la "Puerta de entrada de ciberseguridad de la UIT, y xi) la divulgación y promoción.

[25] www.apec.org

[26] www.bancomundial.org

Referencias

1.- Horacio Fernandez Delpech, “Internet: Su problemática Jurídica”. Editorial Abeledo Perrot. Buenos Aires 2004.

2.- “Los delitos Informáticos en el Código Penal”, Pablo A. Palazzi. Editorial Abeledo Perrot. Buenos Aires 2009.

3.- “Gobernanza de Internet” Asuntos, actores y brechas. Jovan Kurbalija y Eduardo Gelbstein. Publicado por “Diplo Fundation” 2005. Malta.

4.- Código Procesal Penal de la Provincia de Córdoba. Supervisión de Raul Alejandro Gualda. Editorial Alveroni. Decima Edicion 2010.

5.- Constitución de la Nación Argentina. Editorial A-Z Buenos Aires, 16ª Edición, Argentina. 2000.

6.- Ministerio publico Fiscal de Córdoba. www.mpfcordoba.gov.ar

7.- Poder Judicial de la Provincia de Córdoba. www.justiciacordoba.gov.ar

8.- Unidad de respuesta ante incidentes en redes. www.arcert.gov.ar

9.- Jeimy J. Cano. http://www.acis.org.co

10.- Instituto de las naciones Unidas de investigación Interregional de Crimen y Justicia. http://www.unicri.it

11.- Unión Internacional de las telecomunicaciones. www.itu.int

12.- La Comisión Económica para América Latina (CEPAL). www.eclac.org

13.- Asia Pacific Economic Cooperation. www.apec.org

14.- Banco Mundial. www.bancomundial.org