PROYECTO DE LEY

LA LEGISLATURA DE LA PROVINCIA DE ENTRE RÍOS

SANCIONA CON FUERZA DE LEY

ARTÍCULO 1º: La provincia de Entre Ríos, en lo que respecta a su competencia, dispone su adhesión a la Ley Nacional Nº 27.411, por la cual se aprueba el **CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA**, adoptado en la ciudad de BUDAPEST, HUNGRÍA, El 23 de noviembre de 2001.

ARTICULO 2º: Apruébese los puntos 2.5 (2.5.1; 2.5.2; 2.5.3; 2.5.4) del capítulo sobre Recolección de Evidencias Digitales del "Protocolo Unificado de los Ministerios Públicos de la República Argentina: Guía para el Levantamiento y Conservación de la Evidencia" el que como ANEXO I forma parte de la presente.

ARTICULO 3º: Comuníquese el contenido del documento mencionado en el artículo precedente al Superior Tribunal de Justicia de Entre Ríos y al Ministerio Público Fiscal de la provincia de Entre Ríos.

ARTICULO 4º: De forma.

ARTICULO 5º: Comuníquese al Poder Ejecutivo.

AUTOR

CASTRILLON SERGIO

COAUTOR: HUSS JUAN, SOLANAS JULIO, SILVA LEONARDO, REBORD MARIANO, RAMOS CARINA, MORENO SILVIA, FARFÁN MARIANA, CASTILLO VANESA, KRAMER JOSÉ.

FUNDAMENTOS

Honorable Cámara:

Podemos sostener que en este siglo XXI estamos atravesados por una dinámica de constante cambio y devenir acerca de las formas de situarnos y de relacionarnos, en razón de la globalización informática.

Internet es la tecnología decisiva de la era de la información, del mismo modo que el motor eléctrico fue el vector de la transformación tecnológica durante la era industrial.

Esta red global de informática, que actualmente opera sobre todo a través de plataformas de comunicaciones inalámbricas, nos proporciona la ubicuidad de una comunicación multimodal e interactiva en cualquier momento y libre de límites espaciales.

La centralidad de la vida cotidiana de las personas tiene como eje la informática y es deber del estado regularla para seguridad y optimización de derechos y garantías.

Desde la incorporación de mecanismos electrónicos en la vida cotidiana, muchos países comenzaron a modernizar su legislación de acuerdo a las nuevas modalidades ilícitas.

Algunos países incorporaron los delitos informáticos a su normativa mediante la promulgación de leyes específicas en el área, mientras que otros modificaron su legislación para incorporar nuevas figuras.

Es en este contexto, teniendo en cuenta el uso que se hace de la telefonía

móvil en los entornos familiar, empresarial y rural, y considerando el uso limitado de estos aparatos entre niños menores de cinco años, podemos decir que casi toda la humanidad está conectada, aunque con importantes diferencias en cuanto a ancho de banda y a eficiencia y precio del servicio, ubicando a nuestro país como uno de los más débiles en este sentido.

Más aún, ya podemos sostener que la generación T, los nacidos desde 2010 hasta la actualidad, son niños y niñas, que conocen el mundo a través de una pantalla digital y lo que es más importante, táctil.

La hiperconexión, velocidad e instantaneidad son algunas de las palabras que van a acompañar a esta generación y lo que queda de nuestro futuro.

También, estas tecnologías junto con la globalización han permitido un mundo más chico, más cercano e intenso, con muchísimas ventajas que permiten mejorar la calidad de vida de los hombres y mujeres, pero al mismo tiempo, desventajas, sobre todo en la inseguridad, incertidumbre y falta de control.

Las tecnologías de información y comunicación, han cambiado la forma de interrelacionarnos, y particularmente internet, ha modificado las relaciones económicas, políticas, sociales y personales, pero también, el crimen como hecho social, ha originado una nueva forma de criminalidad.

Los cambios experimentados como consecuencia de la utilización de herramientas tecnológicas no sólo hicieron surgir nuevas formas de afectar los intereses sociales, sino también afectaron a los protagonistas del fenómeno criminal: el autor y la víctima.

Es menester destacar que en la actualidad, la mayoría de tipos penales

regulados tanto por el Código Penal de la Nación, tienen directa o indirectamente a la hora de su realización, alguna vinculación con la informática.

Desde un punto de vista criminológico, existen dos enfoques, en cuanto a la naturaleza de este nuevo tipo de fenómeno criminal; el primero de ellos es que los delitos informáticos no son más que delitos convencionales que toman nueva vida a partir del uso de dispositivos informáticos, de servicios y aplicaciones en internet.

La segunda perspectiva afirma que las tecnologías de la información y comunicación, brindan nuevas herramientas para la comisión de delitos inexistentes, como la distribución de virus o programas maliciosos a través de la red, ata- ques a sitios web y la piratería del software.

Lo cierto es que ambos enfoques son ciertos. Existen delitos tradicionales que adquieren nuevas formas a partir de la intermediación de dispositivos automatizados como también nuevas formas delictivas que no serían posibles de cometerse si no existiese un programa de software o archivos digitales presente.

Es por ello, que debemos entender al Ciberdelito como el eje de una pirámide delictiva que como Estado, debemos prever y contener.

Y además, contiene una división casi infinita de particularidades tales como el Ciberacoso, el Ciberbullyng, el Grooming, entre otras, pero que tienen como principal nexo las comunicaciones digitales que permiten la concreción de los mismos.

No obstante, independientemente de la cuestión de fondo, en términos

procesales, todo lo vinculado a evidencias digitales se han convertido en las pruebas conducentes y esenciales para resolver las investigaciones.

Hasta se hace difícil pensar en investigaciones de delitos donde no se cuente con algún aparato digital secuestrado o, algún uso de tecnologías.

A partir de allí, tenemos que proveer al estado de herramientas necesarias para el resguardo y cuidado de intereses sociales (o bienes jurídicos) pero enmarcados en el absoluto respeto de las garantías del debido proceso.

Es por ello, que el Congreso de la Nación adhirió a través de ley Nacional Nº 27.411, al CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, adoptado en la ciudad de BUDAPEST, HUNGRÍA, El 23 de noviembre de 2001 que tuvo como principal objetivo "la necesidad de aplicar una política penal común a los estados miembros y fortalecer la cooperación internacional" y "prevenir actos que pongan en peligro la confidencialidad, la integridad y disponibilidad de los sistemas, redes y datos informáticos tanto así como su abuso, la tipificación penal de los actos, mecanismos y procedimientos para su detección, investigación y sanción y fortalecimiento de la cooperación internacional"

Es así, que el Estado Argentino se hace cargo de la problemática de política penal común destinada a prevenir el delito en el ciberespacio y en particular, a través de la adopción de legislación adecuada y para mejorar la cooperación internacional.

Más tarde, en la misma línea argumental, el Ministerio de Justicia y Derechos Humanos de la Nación, a través de la Resolución 231/2018, en el marco del

Programa Nacional de Criminalística, aprobó el Protocolo unificado de los ministerios públicos de la República Argentina, guía para el levantamiento y conservación de la evidencia, es que se decidió abordar la ciberseguridad y mejorar la forma de prevenir las consecuencias de los ciberdelitos.

Desde nuestra Legislatura, entendemos determinante estar a la altura de las circunstancias y adherir a la ley nacional 27.411, para fijar como prioritario en la agenda política, la procura de trabajar en herramientas para resguardar eficazmente los intereses sociales de nuestra sociedad actual, porque entendemos que en estos contextos se encuentra vulnerable.

Claro está, que ese esfuerzo no debe desatender la protección de las garantías del individuo es su intimidad, privacidad y respeto de su estado de inocencia.

Debemos garantizar estos derechos como Estado, y evitar conflictos sociales que se han suscitado en otros países por la intromisión del Estado en la privacidad informática de sus habitantes.

Tenemos que esforzarnos en proveer herramientas normativas eficaces para proveer de seguridad a nuestra sociedad, evitando todo tipo de legislación de excepción, y con ello, se afecte las garantías del debido proceso y el estado de inocencia.

Por lo que para poder condenar a una persona, como principio rector del derecho penal, es necesario recolectar evidencia que demuestre de manera notoria su participación en el delito del cual se la acusa.

La convicción de la responsabilidad de una persona en un hecho debe

sustentarse en la evidencia y no en los prejuicios.

Es por eso también, la adhesión al Protocolo unificado de los ministerios públicos de la República Argentina, guía para el levantamiento y conservación de la evidencia.

Muchas veces -si no todas- esas evidencias se encuentran en ámbitos propios de la persona, como su domicilio, pero otras hay que investigar profundamente la conectividad internacional, de delitos tales como la Ciberpedofilia.

Por lo que las medidas que se lleven a cabo para obtener aquellas evidencias deben tener el cuidado de no afectar el derecho a las personas a su intimidad.

El principio de eticidad del Estado, nos exige que es el mismo estado el primero en respetar la ley y los valores sociales consensuados.

Es por eso, que en este caso, las garantías tienen como objetivo proteger a las personas de posibles abusos e intromisiones arbitrarias en su espacio personal. Pero también, protegerlos de los constantes peligros a los que los expone la red informática internacional.

Ahora bien, las garantías procesales que protegen la intimidad fueron diseñadas para regular las investigaciones que se llevan a cabo sobre entornos físicos, no en este escenario nuevo de tecnologías y comunicaciones.

Este nuevo escenario, donde el 90 % de las evidencias recolectadas en todo tipo de proceso penal, está vinculado a lo digital. Basta con revisar la jurisprudencia o los medios de comunicación para observar que siempre se secuestran celulares, computadoras, notebook, pendrive. Más, aquellas vinculadas directamente con los delitos informáticos.

Sin embargo, en la actualidad un número importante de inseguridad creciente se registran acerca de ciberdelitos por lo que los estados han decidido proveer de herramientas para salvaguardar bienes jurídicos de la sociedad.

Justamente por lo señalado, se vuelve determinante el levantamiento de los rastros e indicios vitales para una correcta investigación criminal en el marco del debido proceso; este protocolo, permite reducir los márgenes de error en la identificación de los responsables de los delitos, al mismo tiempo que permite una colaboración interjurisdiccional.

Este “Protocolo Unificado de los Ministerios Públicos de la República Argentina: Guía para el Levantamiento y Conservación de la Evidencia” es una forma de hacer efectiva procesalmente la protección material del CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA, para todas y todos los entrerrianos.

En el ámbito de la justicia en general se observan a menudo innumerables casos de pruebas contaminadas, pérdida de datos al momento de recogerlos, rotura de cadenas de custodia, falta de rigurosidad en el levantamiento de la evidencia: entre tantos otros problemas a los que se enfrenta la investigación forense en nuestro país.

Cabe destacar que la problemática de la práctica forense y los errores antes mencionados, no solo ocurren en casos aberrantes, homicidios y/o delitos comunes, sino que, también, en siniestros viales, estafas virtuales muy en boga en la actualidad, donde la confusión, las urgencias, muchas veces hace olvidar que, después de todo, hay que trabajar en encontrar los responsables de lo

ocurrido.

Puede observarse que la piedra angular de la solución que trae este protocolo, reposa en una federalización del marco investigativo, y para ello, resulta vital establecer su desarrollo de una manera pragmática, siempre teniendo presente la mirada unificadora que debe prevalecer.

De esta manera, la unificación viene entonces a atravesar esta crisis de falta de unanimidad en la actuación.

Estas situaciones han llevado a sintetizar sistemáticamente en el protocolo mencionado años de estudio por parte de especialistas nacionales en la materia y tiene como antecedente el Convenio Marco N° 986/10 suscripto entre dicho organismo nacional y el Consejo de Procuradores, Fiscales, Defensores y asesores generales de la República Argentina y el Consejo Federal de Política Criminal quienes impulsaron dicho proyecto federal de creación e implementación de Laboratorios Regionales de Forenses de Alta Complejidad.

Todos los actores de dicho protocolo han asumido el compromiso de desarrollar acciones integrales que robustezcan y profesionalicen el trabajo criminalístico y pericial de los Ministerios Públicos de todas la provincias, proveyendo los instrumentos necesarios para el procesamiento de la evidencia, al momento de transformarse en prueba judicial, con el objetivo de establecer criterios prácticos estandarizados e idóneos para el levantamiento de rastros y evidencias, y para la preservación del lugar del hecho y la escena del crimen, lo que supone un correcto abordaje de escenarios presuntamente delictivos, facilitando la posterior intervención forense.

La complejidad, la vorágine y el constante avance de la informática nos obliga como Estado a estar un paso adelante, mejorando constantemente los medios y herramientas por los cuales asistimos a nuestros investigadores, clarificándoles el protocolo y estableciéndoles pautas claras para la prevención y castigo de delitos.

Es por ello que se presenta la siguiente iniciativa, para incluir en la normativa procesal de nuestra provincia este protocolo realizado por especialistas, y que trata de una manera sistémica el levantamiento y conservación de la evidencia, con el objetivo de que haya criterios unificados para evitar la contaminación de las pruebas no solo para los delitos informáticos, sino para todo investigación.

Por todo lo expuesto, es que pedimos el acompañamiento de nuestros pares.

AUTOR

CASTRILLON SERGIO

COAUTOR: HUSS JUAN, SOLANAS JULIO, SILVA LEONARDO, REBORD MARIANO, RAMOS CARINA, MORENO SILVIA, FARFÁN MARIANA, CASTILLO VANESA, KRAMER JOSE.

ANEXO 1

Se anexa la parte pertinente del Protocolo unificado de los ministerios públicos de la República Argentina: guía para el levantamiento y conservación de la evidencia:

2.5. Evidencias digitales

2.5.1. Principios generales

Las evidencias digitales son elementos tecnológicos que pueden poseer información almacenada en formato digital, como PC, notebook, netbook, tablets, celulares, pendrive, CD, DVD, discos rígidos, servidores, etc. Para aquellas situaciones que involucren procedimientos judiciales en empresas o instituciones de gran envergadura, a priori se procurará obtener información tendiente a conocer las características generales de la infraestructura tecnológica y hardware existente en el lugar del hecho. Las actividades operativas corresponden al personal policial y deben ser efectuadas siguiendo las indicaciones del presente protocolo. La actuación profesional del perito es, principalmente, una actividad de laboratorio y de asesoramiento científico al operador judicial que es responsable de la investigación penal. La pericia informática conlleva tiempos elevados de trabajo y no es posible realizarla sobre grandes cantidades de elementos. Debe evitarse el secuestro masivo de elementos informáticos, en especial CD y DVD, los que solo han de ser enviados a peritaje únicamente si se tienen presunciones con un alto grado de verosimilitud de poseer la evidencia buscada. Cabe aclarar que, de ser posible,

se sugiere realizar, previo al allanamiento, una investigación minuciosa con el objeto de identificar con precisión la ubicación y características técnicas generales de los elementos a secuestrar por medio de inteligencia policial. Respecto a la evidencia digital se deberá identificar claramente qué dispositivos móviles están en uso y a quiénes pertenecen, como así también los que se encontraron apagados, guardados o en aparente desuso. A continuación, se describen los principios generales para la recolección y embalaje de las evidencias digitales halladas en la escena del crimen.

1) Registrar lo que es visible en los dispositivos de salida como pantallas e impresoras y no intentar explorar los contenidos ni recuperar información de una computadora u otro dispositivo electrónico (cámara de fotos, celular, etc.) sin contar con los conocimientos técnicos para realizarlo.

2) No presionar cualquier tecla ni hacer clic del mouse.

3) Verificar si existen discos o CD puestos en unidades.

4) Identificar claramente qué dispositivos móviles están en uso y a quién pertenecen, dar cuenta también de los dispositivos que se encontraron apagados, guardados o en aparente desuso.

5) No encender si se encuentra apagado.

6) Dejar encendido hasta agotar batería.

7) Para apagar, desconectar el enchufe directamente de la red de energía, después desconectar el resto de cables, como la red de datos, monitores, etc.

8) No desarmar el equipo dejándolo sin batería. 9) No abrir la tapa de una computadora portátil si está cerrada.

10) Se realiza algún cambio, registrarlo y justificar.

11) Respetar el orden de volatilidad, estableciendo como criterio preservar la muestra más volátil al principio —como registros, cachés, memoria de periféricos, memoria (kernel, física), estado de las conexiones de red, procesos que se están ejecutando—.

12) Indicar si el material recolectado se encuentra contaminado con residuos biológicos o peligrosos de cualquier tipo.

2.5.2. Pasos en el lugar del hecho, escena del crimen o en allanamiento

1) Separar a las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos. Si es una empresa, se debe identificar al personal informático interno (administradores de sistemas, programadores, etc.) o a los usuarios de aplicaciones específicas que deban someterse a peritaje. Dejar registrado el nombre del dueño o usuarios del equipamiento informático, ya que luego pueden ser de utilidad para la pericia.

2) Obtener, siempre que sea posible, las contraseñas y/o patrones de bloqueo de aplicaciones, tabletas, celulares, etc. para registrar.

3) Fotografiar todos los equipos informáticos antes de moverlos o desconectarlos. Esto es, fotografiar una toma completa del lugar donde se encuentren los equipos informáticos y de las pantallas de las computadoras, si están encendidas. Excepcionalmente, si se debiera inspeccionar los equipos informáticos o material tecnológico en el lugar del hecho, puede ser

conveniente realizar una filmación o bien una descripción del trabajo que se lleva a cabo ante los testigos.

4) Levantar el material informático con guantes descartables, ya que el teclado, monitores, mouse, CD, DVD, etc., pueden ser utilizados para análisis de huellas dactilares, ADN, etc.

5) Si los equipos están apagados, deben quedar apagados; si están prendidos, deben quedar prendidos y consultar con un especialista la modalidad de apagado (en caso de no contar con asesoramiento, proceder a apagarlos desenchufando el cable de corriente desde el extremo que conecta al gabinete informático). Si los equipos están apagados, desconectarlos desde su respectiva toma eléctrica y no del enchufe de la pared. Si son notebooks o netbooks, es necesario quitarles la o las baterías y proceder a secuestrar los cables y la fuente de alimentación. Para el caso de celulares, retirar la batería. En caso de no poder extraer la batería, apagarlo y proteger el botón de encendido con un cartón pegado con cinta para evitar el encendido accidental. Como medida extra de seguridad, se puede activar el “modo avión” antes de apagarlo.

6) De ser necesario, dejar el dispositivo encendido por algún requerimiento específico —por ejemplo: para no perder información volátil colocarlo en una bolsa de Faraday o envolverlo con, al menos, tres capas de papel aluminio—.

7) Identificar si existen equipos que estén conectados a una línea telefónica y, en su caso, el número telefónico para registrarlo en el acta de allanamiento.

8) No realizar búsquedas sobre directorios ni ver la información almacenada en los dispositivos, ya que es posible que se altere y destruya evidencia digital (esto incluye intentar hacer una “copia” sin tener software forense específico y sin que quede documentado en el expediente judicial el procedimiento realizado).

9) Identificar correctamente todo el material tecnológico a secuestrar:

a) Siempre debe preferirse secuestrar únicamente los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadoras, notebooks y discos rígidos externos). Respecto a DVD, CD, pendrives, etc., atento a que pueden encontrarse cantidades importantes, debe evitarse el secuestro de este material si no se tiene una fuerte presunción de hallar la evidencia en estos medios de almacenamiento.

b) Rotular el hardware que se va a secuestrar con los siguientes datos:

i) Para computadoras, notebooks, netbooks, celulares, cámaras digitales, etc.: número del expediente judicial, fecha y hora, número de serie, fabricante, modelo.

ii) Para DVD, CD, pendrives, etc.: almacenarlos en conjunto en un sobre antiestático, indicando número del expediente judicial, tipo (DVD, CD, pendrives, etc.) y cantidad.

c) Cuando haya periféricos muy específicos conectados a los equipos informáticos y se deban secuestrar, deben identificarse con etiquetas con números los cables para indicar dónde se deben conectar. Así como también, fotografiar los equipos con sus respectivos cables de conexión etiquetados.

2.5.3. Registros activos y volátiles de las PC, netbooks y notebooks

TIPO DE MUESTRA	RECOLECCIÓN	PREPARACIÓN	EMBALAJE
Estado de la memoria RAM	Capacidad de los programas cargados. Bloqueos. Porcentaje de uso		
Procesos activos	Uso de CPU. Dependencias de procesos y componentes		
Conexiones de red	Conexiones actuales con otras PC y servidores	Identificación de elementos con respaldo de impresiones, fotografías y actas	No instalar programas en las PC. Realizar las operaciones con los equipos encendidos y cables conectados
Impresiones activas	Cola de impresión local. Documentos sin imprimir. Estado y descripción de los documentos que se están imprimiendo		
Fecha y hora del sistema operativo	Fecha y hora del sistema operativo. Zona horaria. Sincronizaciones con servidores de hora en Internet		
Red de la empresa u organización	Características. Tráfico. Congestión. Bloqueos. Snifers activos. Virus de red		
Papeles impresos	Recolección de papeles impresos en el lugar	Identificación de elementos con respaldo de fotografías y actas	
Conexiones físicas de red	Cableados existentes. Hubs. Suitchs	Identificación de elementos con respaldo de fotografías y actas	No desconectar hasta tanto se recolecte y documente la evidencia

2.5.4. Medios de almacenamiento

<table>
<tr><th>TIPO DE MUESTRA</th><th>RECOLECCIÓN</th><th>PREPARACIÓN</th><th>EMBALAJE</th></tr>
<tr><td>Discos duros de PC</td><td>Descripción del gabinete en el cual está contenido (marca, color, número de serie). Marca y número de serie. Capacidad</td><td rowspan="5">Rotulado. Embalaje en bolsas especiales tipo Faraday o en sobres de papel madera. Precinto de seguridad. Identificación de elementos con respaldo de impresiones, fotografías y actas</td><td rowspan="5">Capturar datos volátiles antes de apagar</td></tr>
<tr><td>Discos duros externos</td><td>Marca y número de serie. Capacidad</td></tr>
<tr><td>Pendrives, CD, DVD, disquetes, otros dispositivos similares</td><td rowspan="3">Marca. Capacidad. Color</td></tr>
<tr><td>Netbooks, notebooks, tablets</td></tr>
<tr><td>Cámaras fotográficas, celulares, mp3, mp4, ipods</td></tr>
</table>

Fuente: Protocolo unificado de los ministerios públicos de la República Argentina: guía para el levantamiento y conservación de la evidencia / Anónimo. - 1a ed . - Ciudad Autónoma de Buenos Aires: Ediciones SAIJ, 2017. Libro digital, EPUB.