LOS ALLANAMIENTOS REMOTOS Y EL USO DE DRONES O ROBOTS*

Diego Stratiotis**

Resumen: *El objetivo del presente trabajo es investigar los allanamientos remotos o virtuales como medida de investigación penal. Se analiza su incorporación a la Ley de Enjuiciamiento Criminal Española, donde se autorizan los registros remotos a distancia, mediante la instalación de un software y en forma secreta. A su vez, se revisan las particularidades de los "hackeos" estatales a través de software espías o maliciosos (malware). También se examina el novedoso uso de drones destinado a la recolección y secuestro a distancia de archivos y documentos digitales almacenados en dispositivos electrónicos. Finalmente, se critica la anomia existente en materia procesal penal en la República Argentina con relación a los allanamientos remotos y se desarrollan los motivos por los cuales se entiende que deben ser incorporados al régimen procesal argentino rápidamente.*

Palabras claves: allanamientos remotos, registros remotos, accesos remotos, *hackeo* estatal, programas maliciosos, drones, libertad probatoria.

§ 1. INTRODUCCIÓN

Mediante el presente artículo analizaré los allanamientos virtuales (en España denominados registros remotos sobre equipos informáticos) los cuales son utilizados para extraer información alojada en un dispositivo electrónico de manera remota y subrepticia.

A tal fin revisaré la modificación a Ley de Enjuiciamiento Criminal española, en la cual, a partir de la Ley Orgánica N° 13/2015[1], se han

* Agradezco profundamente los importantes comentarios y aportes que recibí durante la elaboración del presente artículo del Doctor Marcos Salt, los Ingenieros Gustavo Presman y Pablo Romanos y la Doctora Sabela Oubiña Barbolla.

** Abogado (UCA). Especialista en Derecho Penal (UBA). Especialista en Derecho Administrativo (UB). Docente (UBA).

incorporado diversos medios de investigación tecnológica, entre los que se encuentran los registros remotos a través de la instalación de un *software (spyware)* en el dispositivo electrónico a investigar.

También, me concentraré en las diversas técnicas de *phishing*, la utilización de *malware* y la ejecución de *hacekos*[2] legales por parte de los Estados.

Luego, me concentraré en el estudio de un nuevo desarrollo argentino, mediante el cual a través de drones o robots se puede secuestrar evidencia digital almacenada en un dispositivo electrónico[3], ello se ejecuta efectuando una intrusión secreta en la red inalámbrica de internet que se encuentre utilizando el dispositivo a investigar.

Sentado lo expuesto, revisaré cuál es la situación actual de la legislación procesal argentina con relación a los allanamientos remotos, como así también, cuáles son las ventajas y desventajas que puede implicar la inclusión de medidas de investigación a distancia en causas penales.

§ 2. ALGUNOS CONCEPTOS INFORMÁTICOS PREVIOS

A continuación efectuaré una breve reseña sobre algunos conceptos informáticos que utilizaré a lo largo del presente artículo, cuya comprensión posibilitará una mejor interpretación de los allanamientos remotos, como ser:

---

[1] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

[2] Sobre el termino *hacker*, hispanizado como jáquer, la RAE brinda dos acepciones. En la primera remite al término "pirata informático", al cual define como: "Persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta", y en la segunda acepción se define al hacker como: "Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora".
A los fines del presente artículo se utilizarán los términos *hacker* y *hackeo* estatal en el marco de la segunda acepción, pues mal puede considerarse como un delito a un "*hackeo* estatal" en aquellos países donde se encuentra habilitado legalmente, como así tampoco, puede llamarse ciberdelincuente al *"hacker"* que lo lleva adelante.
A quien accede ilegalmente a un sistema informático o comete delitos informáticos lo llamaré simplemente ciber delincuente, pero no *hacker*.

[3] Denominado Crozono.

a) <u>Evidencia digital</u>: Previo a conceptualizar que es evidencia digital, empezaré por el termino *evidencia*. Al respecto, Taruffo nos enseña que *evidencia* no es lo mismo que *prueba*, ya que *evidencia* (*evidence*) es cualquier elemento o medio de prueba que puede ser utilizado para establecer la verdad de un hecho[4] y *prueba* (*proof*) es el resultado o conclusión.

Es decir, la evidencia son los datos cognitivos e información (Ej.: documentos, datos informáticos o digitales, etc.) y las *pruebas* son las conclusiones o inferencias extraídas a partir de los medios de pruebas relevantes que dan sustento a la verdad de los enunciados[5] sobre los hechos litigiosos que fácticamente ocurrieron en el pasado[6].

Respecto del término *digital*, la RAE ofrece dos acepciones de utilidad para la presente investigación, en la primera lo relaciona a "un dispositivo o sistema: que crea, presenta, transporta o almacena información mediante la combinación de bits" y en la segunda lo define como aquello "que se realiza o transmite por medios digitales. Ejemplo: señal, televisión digital."[7]

Presman expresa que existen muchas definiciones sobre *evidencia digital*, sin embargo destaca que todas ellas tienen como puntos en común "…que se trata de registros que fueron procesados en un dispositivo informático y se encuentran almacenados o fueron transmitidos a través de un medio de comunicación informático."[8]

Sin perjuicio de todo lo expuesto, es frecuente que se utilicen en algunos textos legales los términos evidencia y prueba como sinónimos, por ejemplo, en la Resolución N° 234/2016 del Ministerio de Seguridad de Nación se definió que la "Evidencia digital: es la prueba fundamental en los ciberdelitos.

---

[4] Taruffo, Michele, La Prueba, Marcial Pons, Madrid, 2008, pág. 16 con referencia a Gascón Abellán en su obra "Los hechos en el derecho. Bases argumentales de la prueba", Marcial Pons, 2002 "…en los sistemas procesales modernos no se espera encontrar la "verdad" recurriendo a la adivinación, echándolo a la suertes, "leyendo" las hojas de té, mediante un duelo judicial o por algún otro medio irracional e incontrolable (como los juicios de Dios o algún otro tipo de ordalías medievales), sino sobre la base de medios de prueba, que han de ser apropiadamente ofrecidos admitidos y presentados."

[5] Taruffo, Michele, La Prueba, op. cit., pág. 19 "…Cuando hablamos de la verdad de un hecho, en realidad hablamos de la verdad de un enunciado acerca de un hecho. En consecuencia, lo que se prueba o demuestra en el proceso judicial es la verdad o falsedad de los enunciados sobre los hechos en litigio."

[6] Taruffo, Michelle, La Prueba, op. cit., pág. 35

[7] https://dle.rae.es/digital

[8] Presman, Gustavo Daniel, Cibercrimen II, "La cadena de custodia en la evidencia digital", Editorial BdeF, Buenos Aires, 2018, pág. 304.

Información y datos de valor en una investigación que se encuentra almacenada, es recibida o transmitida por un dispositivo electrónico. Dicha prueba se adquiere cuando se secuestra y asegura para su posterior examen. Normalmente las pruebas consisten en archivos digitales de texto, vídeo o imagen, que se localizan en ordenadores y todo tipo de dispositivos electrónicos."[9]

La confusión o ambigüedad entre los términos *evidencia* y *prueba* puede llevar al error de presentar en juicio a las evidencias digitales (medios de prueba: documento informáticos, archivo digital, etc.) recolectadas por el ingeniero informático como si fueran las pruebas (conclusiones o inferencias) en sí mismas.

La distinción es importante ya que, primeramente, el perito informático, en razón de su especialidad técnica recabará evidencias digital, probablemente sin conocer los pormenores del caso en litigo, y, a partir de ello, esa evidencia digital recolectada será considerada únicamente como prueba, si a partir de una valoración racional de todos los elementos del caso, permite probar la hipótesis planteada sobre los hechos que se investigan.

Es decir, el perito forense recaba evidencia y de la valoración racional de la misma se podría obtener la prueba que sustente la hipótesis planteada sobre los hechos.

La evidencia digital tiene características propias[10] que la diferencian de la evidencia física, como ser:

- *Duplicidad:* la evidencia digital es digital, es decir, se conforma por un conjunto de *bits*, compuesta por un valor binario: cero o uno. Esta característica es clave en el orden a la posibilidad de duplicarla en forma idéntica e indistinguible del original.
- *Intangibilidad:* la evidencia digital no puede ser captada a través de los sentidos, sino a través de complejos procesos informáticos.

[9] Http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm

[10] Dada mi formación como abogado, para el estudio en profundidad de las cuestiones informáticas se recomienda la lectura del experto informático Gustavo Daniel Presman, Cibercrimen II, "La cadena de custodia en la evidencia digital", Editorial BdeF, Buenos Aires, 2018, pág. 304 y siguientes.

Presman nos enseña que es importante distinguir al dispositivo electrónico *(Hardware)* respecto del contenido que almacena *(software).* Muchas veces se identifica al *hardware* como la evidencia digital, pero lo que realmente constituye la evidencia digital son los datos informáticos contenidos en ella.

- *Volatilidad y fragilidad:* los datos electrónicos puedan ser alterados, movidos o borrados en sólo segundos, pueden ser fácilmente manipulados[11].
- *Metadatos:* son los datos que describen a los datos, por ejemplo, a simple vista podemos ver una fotografía o un texto de *word* guardado en un dispositivo electrónico, pero si accedemos a sus metadatos podríamos ver más información, como ser: la ubicación geográfica desde dónde fue tomada una fotografía o la fecha de la última modificación o borrado de un texto, la fecha de creación, horario y demás datos que pueden ser muy útiles para una investigación.

  Según la aplicación o teléfono celular utilizado los metadatos a obtener podrán ser más o menos completos.

  Otro ejemplo de metadatos son los que se encuentran incrustados en los encabezados de los correos electrónicos desde los cuales se pueden obtener direcciones IP, etc.

  Muchas veces los metadatos se encuentran ocultos o no son vistos fácilmente por quien no domina la informática. Su uso en un proceso penal puede ser de gran utilidad para probar los enunciados sobre los hechos controvertidos.

La *evidencia digital* a su vez puede dividirse en tres clases:

1) La de tipo *persistente o de almacenamiento o estática* que es la que se encuentra almacenada en un dispositivo electrónico (Ej.: disco duro, CD, DVD, etc.) y que quedará guardada incluso si se apaga el dispositivo[12].

2) La de tipo *volátil o de procesamiento* que se caracteriza por su inestabilidad, ya que al apagar el equipo informático se perderá.[13] Por ejemplo,

[11] Informe explicativo del Convenio sobre la Ciberdelincuencia (STE núm. 185), puntos 133 y 155.
[12] Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, La Prueba Electrónica, La Ley, Ciudad Autónoma de Buenos Aires, 2019, pág. 91.

el contenido de la memoria RAM permite preservar las últimas actividades que se realizaron en el dispositivo informático.

3) La de *transmisión o tráfico* que representa la información que se transmite a través de la red de comunicaciones (Ej.: llamada mediante aplicación de *whatsapp*). La particularidad de esta evidencia es que se recolecta por el investigador informático para adelante, ya que una llamada no se almacena. El momento de su recolección es durante su tráfico, no es información histórica o almacenada.

Es importante tener en cuenta que las distintas clases de evidencia digital impactarán en la planificación de su recolección en una investigación penal, pues, en los casos de evidencia de tipo *persistente* se puede efectuar una *adquisición estática*, la cual se hará usualmente con el dispositivo apagado ("dispositivo muerto") una vez incautado y en poder del investigador (el ejemplo típico es el del secuestro del dispositivo en un allanamiento tradicional).

Y, por otro lado, en los casos de evidencia del tipo *volátil* o de *transmisión* se hará una *adquisición de tipo dinámica* con el equipo encendido ("dispositivo vivo") y eventualmente conectado a una red (VPN, internet, etc.) (Un ejemplo de ellos pueden ser los allanamientos remotos, podría ser el caso del uso de drones o robots para su adquisición o secuestro).

b) *Cadena de custodia*: Según la Corte Interamericana de Derechos Humanos la *cadena de custodia* consiste en "...llevar un registro escrito preciso, complementado, según corresponda, por fotografías y demás elementos gráficos para documentar la historia del elemento de prueba a medida que pasa por las manos de diversos investigadores encargados del caso"[14].

La cadena de custodia permite registrar la secuencia o camino recorrido por la evidencia desde que fue encontrada, destinada a demostrar el origen, identidad e integridad de la evidencia[15], permite visualizar la trazabilidad de la

[13] Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, op. cit., pág. 91.
[14] Corte Interamericana de Derechos Humanos, "Favela Nova Brasilia Vs. Brasil", 16 de Febrero de 2017.
[15] Di Orio, Ana Haydée, Info Lab, El rastro digital del delito, 2017, pág. 184

misma. No garantiza que la evidencia digital no sea contaminada[16], pero si nos va a permitir controlar en qué momento fue alterada.

Se han desarrollados diversos protocolos o guías de actuación destinados a reglamentar metodologías para garantizar la búsqueda, obtención, preservación y análisis pericial de la evidencia digital; por ejemplo, en la Provincia de Buenos Aires se desarrolló la "Guía Integral de Empleo de la Informática Forense en el Proceso Penal"[17] aprobada por la Procuración General de la Suprema Corte de la Provincia de Buenos Aires (Res. Gral. 483/2016), allí se establecen diversas fases de actuación del informático forense, como ser: *1) Relevamiento e identificación* de los equipos informáticos, dispositivos, etc. útiles para la investigación, *2) Recolección* de los equipos informáticos, dispositivos, etc. *3) Adquisición de datos volátiles* que "…se trata de la obtención de datos existentes en dispositivos encendidos que pueden perderse definitivamente al ser apagado el artefacto", *4) Cadena de custodia y preservación, 5) Adquisición de medios de almacenamiento persistentes* y *6) Labores periciales*.

En particular, dicha guía a la *cadena de custodia y preservación* se la trata por separado, ya que la misma atraviesa a varias de las fases mencionadas (punto 4, identificado en el párrafo anterior)[18].

Asimismo, a la *cadena de custodia y preservación* la referida guía la identifica como "…la secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que esta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia preservando su fuerza probatoria (…) La cadena de custodia comienza desde el momento del hallazgo o recepción de la evidencia y finaliza cuando la autoridad judicial competente decide sobre su destino…".[19]

[16] Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, op. cit., pág. 108.
[17] Info Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense.
[18] Info Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, pág. 12.
[19] Info Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, pág. 23.

Sobre esa definición importa destacar que la cadena de custodia inicia desde el primer contacto y registro sobre la evidencia independientemente del momento de su incorporación al proceso.

c) Copia forense y Hash: Presman nos explica que "…la copia forense es aquella que se realiza *bit a bit* del contenido y validándolo mediante un digesto matemático o función de *hash* con el objeto de asegurar la integridad del contenido binario recolectado."[20]

Hemos visto que una de las características principales de la *evidencia digital* es la duplicidad, consecuentemente la copia forense o imagen forense, a través de *software* específicos, nos permiten obtener copias idénticas de un archivo informático en la cantidad que se desee.

El código de *hash* es una cadena alfanumérica hexadecimal que se genera por la aplicación de un algoritmo que identifica de manera inequívoca el contenido de un documento electrónico determinado, si se realiza un cambio sobre el contenido de ese documento –por más que sea de un *bit*- el código de *hash* cambia en su cadena alfanumérica hexadecimal.

Asimismo, el mismo código de *hash* permite identificar que el original y sus respectivas copias son idénticas, como así también, controlar que la evidencia digital incorporada al proceso será siempre la misma y que no fue modificada (los códigos más utilizados son SHA-1, SHA 256 y SHA 512)[21].

d) *Phishing* y programas espías o maliciosos *(malware)*: el *phishing* es una maniobra llevada a cabo por medios informáticos destinada a robar datos personales, claves de cuentas bancarias, datos de tarjetas de crédito, etc.[22]

El *phishing* consiste básicamente en engañar a alguien, por ejemplo, a través del envío de un correo electrónico o mensaje donde el remitente se hace pasar falsamente por el representante de una institución real (banco, empresa,

[20] Presman, Gustavo, Cibercrimen II, op. cit., pág. 310.
[21] Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, op. cit., pág. 33.
[22] Gris Muniagurria, Pablo H. – Cherñavsky, Nora A. – Moreira, Diógenes A., Sistema penal e informática, Vol. 2, Phishing: abordaje del fenómenos desde la prevención y la investigación, Ed. Hammurabi, Buenos Aires, 2019, pág. 117.

etc.) mediante la utilización de una página falsa a los fines de que el receptor (víctima) introduzca sus datos personales.

Es habitual que la técnica de *phishing* sea utilizada para instalar en el dispositivo de la víctima un programa espía *(malware)* en forma remota y secreta, el *malware* se encargará, por ejemplo, de monitorear comunicaciones y acceder a la información almacenada.

Los programas espías pueden ser utilizados por delincuentes (dirigidos a buscar cualquier blanco vulnerable) o por los Estados (dirigidos habitualmente a blancos específicos), éste último caso ya se ha incorporado en códigos procesales penales de diversos países.

§ 3. PLANTEO DEL TEMA: INVESTIGACIONES REMOTAS Y DRONES

El mundo informático es una nueva realidad que trasciende a los medios de prueba tradicionales, es habitual encontrarnos con allanamientos físicos donde se secuestran los dispositivos electrónicos *(hardware)* para luego, en una segunda etapa, efectuarse un peritaje destinado a acceder a su contenido almacenado *(software)*[23], dichos procedimientos en muchas ocasiones son altamente ineficaces dadas las ya referidas características de la evidencia digital (Ej.: volatilidad, fragilidad, fácil borrado, etc.), como así también la posibilidad de proteger los datos informáticos mediante técnicas de encriptación o claves que dificultan el acceso de terceros.

Las investigaciones penales en Argentina se encuentran frente a dos realidades que funcionan a velocidades distintas; por un lado, los ciberdelincuentes avanzan velozmente en la comisión de delitos a través de herramientas digitales cada vez más sofisticadas y, por otro lado, se encuentran los investigadores penales muy por detrás, entorpecidos por la falta de regulación de medios procesales adecuados que permitan efectuar investigaciones eficaces de ciberdelitos; cuya consecuencia se ve materializada en muchos casos en la extensión y re interpretación forzada, a mi

[23] Sergi, Natalia, Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina, Vol. 3, Buenos Aires, pág. 15 y sgtes.

juicio, del principio de libertad probatoria[24] a los fines de incorporar medidas de investigación no previstas procesalmente.

El Convenio sobre la Ciberdelincuencia o Ciberdelitos (Conocido como convenio de Budapest) al cual la Argentina adhirió a través de la Ley N° 27.411 en el año 2017, promueve a través de su preámbulo la utilización de medios de investigación eficaces en materia de delitos informáticos y su sección 2 se dedica a medidas procesales (Arts.14 a 21).

Con relación a ello, muchos países ya han actualizado sus códigos procesales, por ejemplo, en España en el año 2015 se ha modificado su Ley de Enjuiciamiento Criminal (Ley Orgánica N° 13/2015) incorporando la regulación de diversos institutos vinculados a investigaciones contra el cibercrimen o delitos graves a través de medios informáticos, como ser: registro de equipos informáticos, interceptación de comunicaciones telefónicas y telemáticas, agente encubierto en la red, captación y grabación de imágenes en espacios públicos y privados, como así también, el acceso remoto a dispositivos electrónicos mediante la instalación de *software* (Siendo esta última medida la que aquí interesa).

Sobre los allanamientos remotos[25], Salt destaca que son "…un nuevo mecanismo para acceder a la información contenida en soportes informáticos que, por sus características tecnológicas, parece "no encajar" en ninguna de las normas que prevén los medios de prueba tradicionales lo que ha llevado a algunos autores a caracterizarlos como medios de investigación "híbridos""[26].

Las amplias posibilidades de intromisión por parte del Estado en la vida privada e intimidad de las personas a través del acceso remoto y en forma secreta permite obtener sus datos privados del pasado, presente y predecir situaciones del futuro, como ser: gustos, tendencias, etc. a partir del conocimiento de las páginas *web* visitadas, compras efectuadas, *logs* de

[24] Arts. 134 del Código Penal Procesal Federal y 209 del Código Procesal Penal de la Provincia de Buenos Aires.
[25] Werner, Braian Matías, Sistema penal e informática, Vol. 2, El allanamiento de dispositivos como un nuevo allanamiento de domicilio en la era digital, 2019, pág. 192.
[26] Salt, Marcos, Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, Ad-Hoc, Ciudad Autónoma de Buenos Aires, 2017, pág. 54.

conexión, etc.[27]. El límite o la proporcionalidad de esta medida es una cuestión que debe conjugarse equilibradamente entre el interés público en el esclarecimiento de los hechos delictivos investigados, por un lado, y la intimidad o privacidad de los ciudadanos, por el otro[28].

Es usual que se identifique a los accesos remotos con la utilización de *malware* o programas espías, sin embargo existen otros mecanismos, como Crozono, que permiten el acceso a distancia a un dispositivo (pero, sin la utilización de técnicas de *phishing* ni la instalación de *malware*); ello se ejecuta a través de la intrusión de la red de internet *wi-fi* utilizada por el sospechoso, mediante un *software* preparado para la adquisición remota de evidencia trasladado a través de un dron o robot permitiendo acercarse al objetivo, lo cual permite superar barreras físicas o arquitectónicas sin que el investigador tenga que estar físicamente expuesto pudiendo estar a una gran distancia del dispositivo a investigar, más aún puede estar un operador conduciendo el dron y otro operador en cualquier otro lugar del planeta recibiendo y procesando la información que se obtiene subrepticiamente.

Así las cosas, los drones ya no son únicamente cámaras de fotos o videograbadora que vuelan, su funcionalidad es muy amplia y las ventajas de su uso en investigaciones penales ha crecido exponencialmente.

En razón de todo lo expuesto, no puede negarse que es una ardua tarea la que tienen los legisladores por delante, pues, por un lado, la necesidad de la regulación de institutos procesales destinados a combatir la ciber delincuencia es una realidad insoslayable y, por el otro, son medidas muy intrusivas en la vida privada de las personas; así las cosas, posiblemente se deberá elegir no por la mejor regulación sino por la menos mala[29], pero: ¿cuál será su límite?

Seguidamente y como metodología de análisis, iré de lo general a lo particular, empezaré el presente estudio a partir de las medidas de

[27] Salt, Marcos, Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, op. cit., págs. 128 y siguientes.
[28] Bachmaier Winter, Lorena, Boletín del Ministerio de Justicia español, LXXI, Nro. 2195, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", 2017, pág. 5.
[29] Kerr, Orin S., *Executing warrants for digital evidence: the case for use restrictions o non responsive data*, pág. 11.

investigación informática incorporadas al régimen procesal español, al respecto me detendré en los principios rectores que guían su procedencia y, en especial, en el instituto de los registros remotos, para lo cual describiré qué es un *hackeo* legal a través de *malware* y las técnicas de *phishing* destinadas a acceder al dispositivo del sospechoso, para luego dedicar especial atención a los accesos remotos a través de drones mediante el novedoso procedimiento de intrusión en la red *wi-fi* del sospechoso destinado a la obtención de evidencia digital.

Luego continuaré con el contexto legislativo de los accesos remotos en argentina, su aplicación y los límites al principio de libertad probatoria.

§ 4. ESPAÑA: INCORPORACIÓN DE MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

a) Principios generales de procedencia

La reforma a la Ley de Enjuiciamiento Criminal española [30] además de incorporar las ya referidas medidas de investigación tecnológicas, establece principios generales de procedencia para la aplicación de las mismas en virtud de la extrema injerencia que pueden provocar en la intimidad de las personas, en ese orden el artículo 588 bis "a"[31] de la Ley de Enjuiciamiento Criminal

[30] Ley Orgánica 13/2015 de fecha 5 de Octubre.

[31] Artículo 588 bis a. Principios rectores.
1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.
2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.
3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.
4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:
a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o
b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.
5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la

española estipula que siempre debe mediar una autorización judicial habilitante con sujeción a los principios de especialidad, idoneidad, excepcionalidad y proporcionalidad, los cuales además fueron definidos expresamente por el legislador.

Con anterioridad a la entrada en vigencia de la mentada reforma, el Tribunal Constitucional español ha destacado como presupuestos generales de procedencia para las medidas sumamente intrusivas en la intimidad de las personas, los siguientes: un fin constitucionalmente legítimo; que la medida limitativa del derecho se encuentre prevista en la ley; una resolución judicial motivada como regla general y la estricta observancia al principio de proporcionalidad.[32]

Asimismo, dicho Tribunal ha destacado la importancia del juicio de proporcionalidad, para lo cual ha considerado como requisitos del mismo diversos principios recogidos por el legislador español en el referido artículo 588 bis "a"; en ese orden, a través del fallo STC 207/1996 ha expresado que "…para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple las tres condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)."[33]

A continuación reseñaré los mentados principios, incorporados a través del artículo en comentarios, a saber:

- *Principio de especialidad:* mediante este principio se propicia que la medida se encuentre vinculada a un delito concreto y se eviten medidas con fines preventivos o para descubrir delitos o despejar

gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

[32] STC 70/2002, de 3 de abril.

[33] STC 207/1996, de 16 de diciembre, STC 89/2006, de 27 de marzo, entre otros.

sospechas, es decir, sólo pueden ser utilizadas las medidas sobre una base objetiva y no sobre sospechas generales[34].

- *Principio de idoneidad:* relativo a aspectos concretos, como ser: el ámbito *objetivo* (medios de almacenamiento o examen de datos o contenido); *subjetivo* (sujetos concernidos)[35] y la *duración* (plazo de duración de la medida), los cuales se vinculan a la utilidad de la medida (ponderación de la relación entre los datos y las medidas a los fines de determinar si se podrán obtener las pruebas buscadas)[36].

- *Principios de excepcionalidad y necesidad:* mediante los cuales se justifica una medida en aquellos casos que no haya una menos gravosa y cuando la falta de utilización de esa medida dificulte gravemente el resultado de la investigación.

- *Principio de proporcionalidad:* en sentido estricto, el juicio ponderativo es proporcional si tomando en consideración todas las circunstancias del caso, se logra determinar que el sacrificio de los derechos e intereses afectados (afectación de los derechos constitucionales del sujeto investigado) no es superior al beneficio para el *interés público* y de terceros (esclarecimiento de los delitos).

  El legislador específicamente establece en el artículo en comentario que la valoración del *interés público* se basará en la "…gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho."

Dichos principios son una guía central para el juez, es notable el esfuerzo efectuado por el legislador español al definir los mismos en el texto legal, lo cual revela la especial atención y cuidado con la que deben ser

[34] Bachmaier Winter, Lorena, op. cit., con cita del Tribunal Constitucional en su sentencia 253/2006, 11 de septiembre.
[35] Rodríguez Lainz, José Luis, Sobre la ley orgánica de modificación de la LECRIM para el fortalecimiento de las garantías procesales: la regulación de las medidas de investigación tecnológica, pág. 9 y siguientes.
[36] Bachmaier Winter, Lorena, op. cit., Pág. 15.

autorizadas y ejecutadas las medidas de investigación tecnológicas, ya que es un avance muy importante por parte del estado en la vida íntima de los ciudadanos.

En otro orden, en cuanto al procedimiento para la solicitud de una medida de investigación tecnológica, el juez las podrá acordar: 1) De oficio, 2) a instancia del Ministerio Fiscal o 3) de la policía judicial (Art. 588 bis “b”).

En los dos últimos casos la solicitud deberá contener ciertas características, como ser: descripción del hecho, identidad del investigado, razones que justifiquen la medida, extensión de la medida, etc.

Luego, el juez de instrucción autorizará o denegará la medida solicitada mediante auto motivado. En caso de autorización, la resolución judicial deberá contar al menos con diversos extremos, como ser: identificación del hecho punible objeto de la investigación, calificación jurídica, indicios racionales que justifican la medida, identidad de investigados (en caso de ser conocidos), extensión de la medida, alcance, motivación relativa al 588 bis “a”, duración, forma y periodicidad, finalidad de la medida y secreto del sujeto obligado en llevar la medida, principalmente (588 bis “c”).

Las actuaciones relativas a las medidas serán secretas (588 bis “d), podrán ser prorrogadas (588 bis “e” y “f”), el juez de instrucción será informado sobre los resultados de la medida para su control (588 bis “g”), se podrán acotarse las medidas aun cuando afecten a terceras personas (588 bis “h”), la utilización de la información obtenida en un procedimiento distinto y descubrimientos causales se remite a la regulación del 579 bis de la Ley de Enjuiciamiento Criminal (588 bis “i”) y el juez será quien ordene el cese de la medida (588 bis “j”) y quien ordenará la destrucción de registros (588 bis “k”).

b) Incorporación de los registros remotos

La incorporación de los registros remotos como medida investigativa al procedimiento criminal español fue una de las grandes novedades, ello cubrió

un vacío normativo que ya se encontraba previsto en otros países de Europa[37]; como antecedente jurisprudencial en el año 2011 el Tribunal Constitucional español ya había destacado a los accesos remotos como un posible medio técnico de injerencia en el contenido de un ordenador personal[38].

Su regulación se encuentra establecida en los artículos 588 *septies* "a", 588 *septies* "b" y 588 *septies* "c" de la Ley de Enjuiciamiento Criminal.

El Artículo 588 *septies* "a" establece que:

> 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
>
> a) Delitos cometidos en el seno de organizaciones criminales.
>
> b) Delitos de terrorismo.
>
> c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
>
> d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
>
> e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

[37] Proyecto de ley orgánica de modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Exposición de motivos. 13/03/2015. Sitio Ministerio de Justicia español: https://www.mjusticia.gob.es/es/ElMinisterio/GabineteComunicacion/Documents/1292427344734-PLO_modifica_LECrim_CM_13032015_WEB_0.pdf

[38] STC 173/2011, de 7 de noviembre.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

c) Acerca de la instalación de un *software.* Programas maliciosos *(malware)*

El referido artículo prevé la instalación de un *software (spyware)* que permita el acceso a un dispositivo electrónico en forma remota, telemática y sin conocimiento de su titular.

La utilización de un *software* a tales fines es la realización de un *hackeo* estatal, su ejecución implica la instalación de un virus *(malware)* en el dispositivo electrónico a investigar, lo cual implica recurrir a las "…mismas herramientas que los *hackers o crackers* (entendidos como quienes acceden sin autorización a un equipo o sistema), lo cierto es que las herramientas estatales deben cumplir con una serie de requisitos adicionales que las diferencian de los cibercriminales para crear *bootnets* o sustraer dato privados.

Ello así, desde que el *malware* de estos últimos se dirige contra blancos "de oportunidad" (es decir, cualquiera que aparezca vulnerable), mientras que el estatal tiene objetivos específicos. Esto demanda el uso de herramientas de interceptación especializada, cuyo funcionamiento debe superar el estándar meramente "probabilístico de los típicos *exploit* ilegales. En efecto, el *malware* estatal debe tener una alta probabilidad de comprometer exitosamente el equipo de su objetivo sin alterarlo y sin perturbar el funcionamiento de ese equipo ni de ningún otro. Además, debe permitir que quienes lo operan confirmen rápidamente si ha tenido éxito o no, que se lo controle durante el tiempo que dure la intervención legalmente autorizada y que pueda ser eliminado sin dejar rastros una vez que aquella concluya"[39].

Un *exploit* es un programa o código que "explota" una vulnerabilidad (defecto o debilidad de un sistema o de parte de él) para aprovecharla. El *exploit* no es un código malicioso (*malware)* en sí mismo, habitualmente se lo utiliza como un componente dentro del *malware*. Los *malware* generalmente utilizan los *exploit* como "llaves" para acceder a un sistema vulnerable. Existen diversos tipos de *exploit* dependiendo las vulnerabilidades. Las vulnerabilidades más valiosas son las *Zero Day* (día cero) por ser desconocidas para el fabricante del programa y no haber sido mitigadas por un parche[40].

El *exploit* puede ser enviado a la potencial víctima a través de diversos vectores de ingreso, como: un correo electrónico o *link* de acceso a un archivo

[39] Blanco, Hernán, Tecnología Informática e investigación criminal, Ciudad Autónoma de Buenos Aires, La Ley, 2020, pág. 103. Con cita de Bellovin, Steven M. – Blaze, Matt – Clark, Sandy – Landau, Susan, "Going bright: Wiretapping without weakening communications infraestrcuture", en IEEE Security & Privacy, vol. 11, Nro. 1, 2013, Págs. 62/72.

[40] Fuente: Segu info (https://www.segu-info.com.ar/malware/exploit).

o mensaje SMS, entre otros[41], las cuales requieren engañar al usuario o propietario del dispositivo para obtener su "*click*" y lograr así el acceso subrepticio a sus datos informáticos.

Por su parte, los *malware* son códigos informáticos utilizados subrepticiamente, para infectar equipos, perjudicar el funcionamiento de los mismos o robar información con un móvil económico (Ej.: encriptación de datos a cambio de dinero)[42].

Un *software* judicial no tiene ninguno de estos objetivos dañinos, ya que no se encuentran orientados a infectar equipos o perjudicar su funcionamiento, como así tampoco, a robar información. Su objetivo es obtener evidencia en el marco de un proceso penal. No obstante, esta novedosa técnica de investigación judicial se encuentra basada en el uso de programas maliciosos[43].

El *phishing* es la mecánica montada para lograr el *"click"* del usuario, esta técnica es utilizada para el envío de *exploits y malwares*. Litvin define al *"Phishing"* haciendo un paralelismo con el *"Fishing"* que significa "pescar" en inglés, al respecto el "pescador" (cibercriminal o Estado) utiliza como *línea para pescar* un correo electrónico o mensaje de chat y sus *anzuelos* son los archivos adjuntos listos para ser *clickeados* por la *presa* (usuario o propietario del dispositivo), cuya atención fue previamente captada por un *señuelo* incorporado al correo o mensaje enviado, el cual puede ser: noticias sobre famosos, multas de la policía, facturas electrónicas, situaciones que generan alarmas, etc.[44].

El señuelo surge de la ingeniería social (conocida como arte del engaño) efectuada por ingenieros sociales o ciberdelincuentes, es el conjunto

---

[41] Blanco, Hernán, Tecnología Informática e investigación criminal, op. cit., pág. 105 y sgtes.

[42] Fuente: Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad español (INCIBE) (Https://www.osi.es/es/actualidad/blog/2016/10/11/malware-cual-es-su-objetivo-y-como-nos-infecta).

[43] Salt, Marcos, Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, op. cit., pág. 56.

[44] Litvin, Jorge Luis, Hackeados. Delitos en el mundo 2.0 y medidas para protegernos, 2020, pág. 12.

de trucos y estrategias destinados a manipular y captar la atención del usuario o propietario del dispositivo para que actúen cómo los criminales quieren[45].

Con relación a ello, Salt destaca las amplias ventajas de las que puede gozar un Estado al utilizar herramientas oficiales, como puede ser el correo electrónico de una dependencia gubernamental, para acceder subrepticiamente al dispositivo del sospechoso, pues lo usual debería ser que no se desconfíe de los mismos[46].

Al respecto, Blanco destaca que la mecánica del *"phishing"* es probabilística al utilizar un mensaje genérico (metodología equivalente a la pesca con red) y que la variante más efectiva es el *"spear phishing"* (metodología equivalente a la pesca con lanza) consistente en el diseño de un mensaje específico (Ej.: correo electrónico) que contiene el *malware* para engañar a un objetivo determinado[47].

Dado que existen distintos tipos de programas maliciosos, a continuación haré una breve identificación de los mismos[48]:

- *Spyware:* virus destinado a recopilar información de manera fraudulenta sobre navegación del usuario, datos personales y bancarios. Ej.: virus *Keyloggers* que sirven para registrar las teclas pulsadas y obtener todo tipo de información (usuarios, contraseñas, conversaciones, etc.).

- *Gusanos:* virus con capacidad para replicarse entre diversos dispositivos electrónicos. Causa grandes errores en la red por un consumo anormal del ancho de banda.

---

[45] Https://www.osi.es/es/actualidad/blog/2016/03/01/conociendo-que-es-la-ingenieria-social-fondo

[46] Salt, Marcos, Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, op. cit., pág. 66.

[47] Blanco, Hernán, Tecnología Informática e investigación criminal, op. cit., pág. 107.

[48] Información obtenida de la OSI (Https://www.osi.es/es/actualidad/blog/2016/10/11/malware-cual-es-su-objetivo-y-como-nos-infecta - https://www.osi.es/es/actualidad/blog/2020/05/06/principales-tipos-de-virus-y-como-protegernos-frente-ellos - https://www.osi.es/es/actualidad/blog/2018/03/01/cuales-son-las-principales-amenazas-de-apps-maliciosas-en-moviles-0)

- *Troyano:* se presenta como un *software* aparentemente legítimo (Ej.: *app* de apariencia legítima e inofensiva), pero que al ser ejecutada permite al atacante acceder y controlar remotamente el dispositivo infectado. Pone a disposición del atacante todos los datos informáticos almacenados en el dispositivo. Permite robar información.

- *Troyanos bancarios:* Son una mezcla de los troyanos y *keyloggers* y se exteriorizan a través de una *app* que aparenta ser de una entidad bancaria, pero en la realidad no lo es. Permite robar datos bancarios.

- *Ransomware:* software malicioso que se transmite como lo hace un troyano o gusano, pueden estar camuflados a través de una *app*, correo electrónico, etc. Sirven para controlar el dispositivo infectado, bloquearlo y/o cifrar la información almacenada, todo ello para pedir al propietario o usuario un pago como rescate.

- *Adware:* software que ofrece publicidad no deseada. En algunos casos se ocultan detrás de otra programa para que, sin consentimiento del usuario, cuando éste hace un *click* en un programa determinado sin darse cuenta está haciendo *click* en una publicidad.

- *APT (Advanced Persistent Threat)* o amenaza persistente avanzada: Tipo de ataque que combina varias vulnerabilidades y ataques a la vez para conseguir sus objetivos. Por ejemplo, los atacantes utilizan perfiles falsos a través de internet (Ej.: uso a través de redes sociales) para conseguir mediante ingeniería social engañar a sus víctimas, se contactan con ellas (Ej. a través de chats) para luego indicarles que se instalen aplicaciones falsas a través de las cuales infectan un dispositivo electrónico con un troyano.

Por otro lado, en lo relativo al *hackeo* estatal es muy interesante el análisis efectuado por Blanco, quien destaca que se divide en cuatro: 1) Envío *(delivery)*: envío del *exploit* por internet (Ej.: mensaje de correo o mensaje SMS) o en forma física, 2) Intrusión *(exploitation)*: aprovechamiento de la vulnerabilidad a través del *exploit* para superar defensa e instalar el programa malicioso, 3) Ejecución y 4) Reporte *(reporting)*.

La utilización del *hackeo* estatal mediante la utilización de *malwares* tiene abundantes ventajas respecto de los allanamiento tradicionales para la obtención de evidencia digital dadas las características ya descriptas de los datos informáticos (volatilidad, fragilidad, etc.) y las barreras de seguridad como es la encriptación de datos y claves, como así también, el beneficio de obtener información en tiempo real y a distancia.

§ 5. EL REGISTRO REMOTO A TRAVÉS DE DRONES O ROBOTS

No obstante lo expuesto, la técnicas de investigación avanzan a diario, en Argentina se ha desarrollado una nueva forma de acceso remoto que no requiere de la instalación de programas espías, la forma de acceder al dispositivo del sospechoso es a través de la red de internet *wi-fi* que se encuentre utilizando, mediante un *software* incorporado a un dron o robot (proyecto denominado Crozono), el cual permite en forma automatizada la adquisición de evidencia digital forense a distancia superando barreras arquitectónicas[49].

A través de Crozono y desde un dron se accede a la información que un sospechoso está generando desde su computadora prendida (es decir, “viva”). Información que puede ser muy valiosa y que con sólo apagar el dispositivo electrónico podría perderse (Ej.: datos alojados en la memoria RAM, *web sites* visitados, *log* de conexión, etc.); también se podrá acceder a aquellos datos que se encuentran almacenados en la memoria permanente.

La representación gráfica de “viva” es importante, ya que, Crozono no puede encender o apagar el equipo investigado, incluso no puede volver a capturar esa misma información o rastrear ese *log* de conexión en una oportunidad posterior si fue borrado o apagado el equipo. Sí podrá repetir el mismo procedimiento, pero la volatilidad de la información hace que ese hallazgo, posiblemente, sea único.

[49] Toda la información técnica sobre Crozono me ha sido propiciada por uno de sus creadores, Ing. Pablo Romanos, quien me extendió diversos artículos informáticos y con quien mantuve diversas conversaciones destinadas a comprender su funcionamiento.

En este artículo utilizaré como ejemplo a Crozono por dos motivos principales, es un desarrollo concreto que ya ha sido probado y es reconocido internacionalmente y, además, es sumamente novedoso o disruptivo ya que permite el acceso remoto a la información del sospechoso sin la aplicación de técnicas de *phishing* (de momento) o instalación de *malwares* en los dispositivos electrónicos del sospechoso.

Crozono en su esencia busca y se aprovecha de las vulnerabilidades de una conexión inalámbrica de internet para acceder al contenido que se encuentra alojado en un dispositivo electrónico; por ejemplo, aprovecha que frente a cualquier corte de una conexión al servicio de red, automáticamente los dispositivos electrónicos que estaban conectados intentan reconectarse, para ello se dispara en forma automatizada una "negociación" de claves y contraseñas entre el dispositivo electrónico (cliente) y el servidor o proveedor de internet para otorgarle nuevamente la ruta de *wi-fi*. Sobre esta "vulnerabilidad" lo que hace Crozono es provocar intencionalmente el corte de la conexión para aprovecharse de ese procedimiento de reconexión y capturar así la clave y contraseña del cliente que quiere acceder a la red, de este modo Crozono accede a la red en la que se encuentra navegando el dispositivo que se pretende investigar.

Son tres fases o capas las que atraviesa Crozono en una investigación: 1) *Explorer*, 2) *Auditor* y 3) *Forensic*, las cuales profundizaré a continuación:

1) *Crozono Explorer:* dentro de esta fase se efectúa inicialmente una etapa de *reconocimiento* centrado en la recopilación de información del espectro radioeléctrico a investigar a los fines de identificar puntos de acceso inalámbricos, cámaras IP, dispositivos IoT, etc. vinculados la seguridad y ubicación geográfica.

Dentro de esta fase se genera un "mapa de calor" cuyo objetivo es encontrar el camino más simple para efectuar la intrusión a la fuente inalámbrica.

Luego continúa una etapa de *procesamiento* donde se procesan datos de la cobertura y seguridad de la infraestructura.

Y, finalmente, se emite un reporte del cual va a surgir el recorrido realizado por el dron, los potenciales vectores de intrusión, tipos de dispositivos, potencia de emisión, nivel de seguridad, etc.

2) *Crozono Auditor:* en esta etapa Crozono producirá auditorías de seguridad automatizadas dirigidas a una red y tomará decisiones –sin requerir la interacción directa del auditor- en base a parámetros pre-establecidos.

En esta etapa Crozono provocará la interrupción de la red e intentará captar la clave y contraseña del cliente que quiere reconectarse al servicio, la meta es introducirse en la red inalámbrica y abrir una conexión reversa hacia el auditor de Crozono a través de la conexión local de internet de la red que es el objetivo. Esto también permitirá descubrir otros equipos de la red y lanzar diversas acciones ofensivas.

También se producirá aquí la copia de todas las evidencias y detalles que resulten necesarios para la investigación a los fines de lograr su reproducción y explicación procedimental en juicio.

Si no se encuentran redes *wi-fi* en las proximidades la ejecución terminará.

3) *Crozono Forensic:* el objetivo de esta etapa es el registro y secuestro de datos informáticos para ser utilizados como evidencia digital.

A los fines de asegurar la integridad, confidencialidad y disponibilidad de los datos informáticos obtenidos, como así también, permitir detallar el procedimiento seguido (cadena de custodia) la metodología empleada es la establecida según estándares internacionales ISO/IEC 27037 e ISO/IEC 27042.

Crozono permite acceder a la totalidad de los datos de tráfico y de contenido relacionados a un dispositivo electrónico, Pablo Romanos destaca que la forma más segura o respetuosa de los derechos a la intimidad o privacidad se da cuando la orden judicial que autoriza la intrusión limita claramente los objetivos de búsqueda, por ejemplo, en el caso de estar buscando determinadas imágenes de pornografía infantil que hayan sido previamente *hasheadas*, el objetivo sería entrar remotamente a determinada

red para acceder a un dispositivo en la búsqueda de ese *hash*[50] concreto y salir.

El mecanismo aplicado por Crozono no permite copiar toda la información o datos informáticos que se encuentre almacenados en un dispositivo electrónico, efectuar una tarea de tal magnitud en aquellos dispositivos donde se encuentre almacenada una gran cantidad de información es prácticamente de imposible realización dado que no alcanzará el ancho de banda, la ventana de tiempo otorgada judicialmente para realizar la medida es limitada y el posterior procesamiento de infinitas cantidades de información resulta ser generalmente infructuoso; en concreto el punto es que la búsqueda este orientada a lo relevante y no a cualquier cosa.

Según el tipo de conducta delictiva a investigar, Crozono cuenta con 4 perfiles tipificados: Pornografía infantil, Fraude Informático, Propiedad Intelectual y Daño Informático.

En cada uno de ellos existe una automatización independiente destinada a buscar datos específicos, por ejemplo, en el caso de Pornografía Infantil el proceso de identificación implica la búsqueda, el reconocimiento y la documentación vinculada a evidencia digital potencial.

A los fines de garantizar la preservación de la evidencia obtenida Crozono efectuará cálculos de integridad *(hashes)*, exportación de resultados, retorno de historiales de comandos ejecutados.

Este último punto es muy importante en cuanto a la cadena de custodia y la integridad de la evidencia digital obtenida a partir de su copia o duplicación, pues, como hemos referido más arriba la posibilidad de acceder a un equipo "vivo" sería un buen avance en investigaciones penales a los fines de obtener evidencia digital que podría perderse rápidamente, sin embargo una mala

[50] Lic. Nilles, Gerardo y Lic. Silva, Gastón, Pericias informáticas para casos de pornografía infantil, SID 2016, 16º Simposio Argentino de Informática y Derecho, sobre los hashes refieren que: "La principal desventaja es que pequeñas modificaciones en un archivo (un bit) generan valores de hash distintos. Esta técnica deja de ser útil si la imagen buscada sufrió alguna modificación en forma o tamaño." y destacan otros mecanismos de identificación como puede ser la utilización de "Huellas digitales de datos" o "Photo DNA el estándar creado por Microsoft"
(http://sedici.unlp.edu.ar/bitstream/handle/10915/58301/Documento_completo.pdfDFA.pdf?sequence=1&isAllowed=y)

técnica de extracción o manipulación de la evidencia digital haría caer la investigación dictándose su nulidad[51].

[51] La "Guía Integral de Empleo de la Informática Forense en el Proceso Penal" (Aprobada por Resolución 483/16 del Ministerio Público Fiscal de la Provincia de Buenos Aires) establece los siguientes criterios para la adquisición de datos volátiles:

" Aseguramiento:

- Los datos volátiles requieren recaudos específicos para su aseguramiento, dada su especial fragilidad. Se ha de neutralizar o, cuanto menos, minimizar todo riesgo de eliminación o alteración que puede provenir de factores ambientales (especialmente electromagnéticos), de la acción de terceros (presencial o remota) y/o de las propias prácticas desplegadas durante el procedimiento.
- La necesidad de aseguramiento persiste durante todo el proceso de obtención de los datos.

Inspección:

- Se deben llevar a cabo las medidas pertinentes de inspección pasiva (fotografiado y descripción de pantallas, conexiones y dispositivos de red, etc.).
- Según las circunstancias del caso, se accederá a los menús, aplicaciones y archivos activos, para su descripción y captura fotográfica, consignando asimismo la fecha y hora que registra cada dispositivo, y la fecha y hora de la inspección. En todo momento se respetarán los principios de actuación referidos a la manipulación, alteración y/o destrucción de datos.

Manipulación, alteración y/o destrucción de datos:

- Debe procurarse la menor alteración y/o destrucción de datos informáticos.
- En la medida de lo posible, toda alteración de los sistemas debe estar prevista de antemano. El EA debe asegurarse de contar con directivas o criterios claros respecto de cuáles son las pruebas de carácter prioritario.
- Ante situaciones no previstas, se deberá consultar al director de la investigación (Art. 248 del CPP Prov. Bs. As.).
- Debe precisarse en forma documentada en qué ha consistido la alteración, y cuáles son sus efectos sobre el material probatorio adquirido (datos volátiles) y/o sobre la evidencia contenida en medios de almacenamiento persistentes.

Orden de levantamiento de datos:

- El orden en que serán levantados los datos dependerá del previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información.
- Debe tenerse en cuenta que probablemente existan otros datos importantes en sistemas dispositivos periféricos (*router, modem, switch, hub, etc*.).
- Generalmente, será útil recuperar los siguientes datos del sistema en tiempo real: fecha y hora del sistema (contrastada con la hora oficial), procesos activos, conexiones de red, puertos TCP y UDP abiertos, usuarios conectados remota y localmente.

Identificación de usuarios:

- Cuando las circunstancias del caso lo tornaren conveniente, el EA sugerirá al responsable del procedimiento la identificación de las últimas personas que utilizaron el dispositivo y/o de quienes habitualmente tienen acceso al mismo.

Acceso a datos:

- Si especialistas de otra área están buscando evidencia material (huellas digitales, ADN, etc.) y el tipo de dispositivo lo admite, puede ponderarse el empleo de artefactos inalámbricos (mouse, teclado, etc.) para acceder a los datos. En caso de duda, se consultará al director de la investigación.
- Cuando las circunstancias del caso lo aconsejen, se consultará al director de la investigación acerca de la alternativa de poner en estado de hibernación los sistemas de un dispositivo y efectuar su recolección.
- Si se advirtiere que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal, etc., se efectuará consulta al responsable del procedimiento acerca de los límites legales que pudieren existir para la captura de la información.

Registro, documentación y validación:

- El proceso técnico de extracción de información debe documentarse conforme las disposiciones relativas a la fase de recolección, indicando especialmente las herramientas utilizadas y los resultados obtenidos.
- Se adoptarán los principios de cadena de custodia al soporte de la información adquirida. Se sugiere obtener un hash para posterior validación, que será consignado en el acta pertinente, con mención de la fecha, hora, lugar, dispositivo de origen, y EA interviniente.

§ 6. LA AUTORIZACIÓN JUDICIAL DE UN REGISTRO REMOTO ¿CUÁLES SON SUS LÍMITES?

Hasta aquí hemos vistos distintos aspectos del mundo informático y, en especial, accesos remotos, como ser: *hackeo* legal, *exploit, malware,* técnicas de *phishing,* ingeniería social, etc., ahora bien, con relación a la resolución judicial que autorice un registro remoto, el artículo 588 *septies* "a", en su punto 2 "b" de Ley de Enjuiciamiento Criminal establece que el juez deberá especificar:

> "El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información."

A mi juicio es muy importante que se determine el alcance de la misma y principalmente que se determine qué se busca en el dispositivo del sospechoso, sin embargo ¿qué nivel de especificación se lo podría exigir a un juez respecto de cómo se procederá al acceso y aprehensión de los datos o archivos, como así también, sobre el software a utilizar?

En especial las investigaciones informáticas son muy dinámicas, dados los constantes avances y cambios tecnológicos se encuentran abiertas a diversos escollos o sorpresas que son difíciles de prever en su totalidad en muchas ocasiones por los propios expertos informáticos, asiduamente aparecen nuevos *exploit*, vulnerabilidades, parches, etc., a lo cual deben sumarse las habilidades de los ciberdelincuentes para desarrollar mecanismos de ingeniería inversa destinados a detectar *hackeos* legales e intentar sacar provecho de los mismos una vez advertidos, lo cual requiere de la experiencia del perito informático o fuerzas de seguridad para resolver la cuestión durante la realización de la medida y evitar su fracaso.

- Deberá completarse el Acta de Levantamiento de Evidencia Digital (LED). Al respecto, ver fase de Cadena de Custodia."

En ese particular contexto, creo que las exigencias planteadas por el legislador español serán de difícil cumplimiento si se esperan autorizaciones judiciales (conf. art. 588 *septie*s “a” pto. 2 “b”) minuciosas, dónde un juez deba especificar o determinar acabadamente la forma en la que se procederá al acceso de los datos y qué *software* se utilizará (como ser: tipo de *exploit* a utilizar, tipo de vulnerabilidad a atacar, tipo de técnica de *phishing* a realizar, etc.) en definitiva todas estas cuestiones terminarán dependiendo de lo que el perito experto en informática o las fuerzas de seguridad especializadas le indiquen al juez que deba especificar en su orden, con independencia de los altos conocimientos informáticos que los magistrados puedan adquirir.

Quizás una posible solución a esta situación es no exigir a los jueces un alto nivel de especificidad técnica en el contenido de las resoluciones judiciales mediante la cuales se aprueba un registro remoto, todo ello debería ser exigido y especificado en forma orientativa pero no taxativa, pues no necesariamente exigir más significará que las fundamentaciones sean mejores, son muchas las leyes que resultan loables en sus exigencias pero que en la práctica son de imposible cumplimiento[52] y se terminan materializando en resoluciones judiciales ambiguas que luego generan más confusión y planteos de nulidades.

Ello, sin perjuicio de la debida motivación de la orden judicial con plena sujeción a los principios rectores establecidos en el ya visto artículo 588 bis “a” de la Ley de Enjuiciamiento Criminal (especialidad, proporcionalidad, idoneidad, etc.) y, principalmente, la limitación del alcance de la medida, pues, dado el alto nivel de intrusión en la vida privada al que puede acceder el Estado mediante un registro remoto, es necesario que se determine antes de iniciar la medida qué se quiere buscar y se eviten criterios amplios de búsqueda como “todo aquello de interés para la causa”.

No obstante lo expuesto hasta aquí, a mi juicio la principal atención debería concentrarse en el minucioso control *ex post* de la cadena de custodia, que refleje el registro en forma completa y detallada de todos las tareas efectuadas por los informáticos/programas y el movimiento/manipulación de la evidencia. De este modo, las partes podrán controlar la integridad y resguardo

[52] Bachmaier Winter, Lorena, Boletín del Ministerio de Justicia español, LXXI, Nro. 2195, 2017, pág. 28.

de la evidencia obtenida. Lo cual debería estar definido en forma clara en protocolos de actuación redactados por equipos multidisciplinarios (conformados por expertos informáticos, juristas y personal operativo de las fuerzas de seguridad) en los que se definan los aspectos básicos a tener en cuenta en las tareas de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales, en miras a garantizar el registro de cada paso vinculado a la manipulación de la evidencia.

§ 7. CORREO ELECTRÓNICO: ¿DATOS DE ALMACENADO O COMUNICACIÓN?

Como hemos visto, el objetivo de los registros remotos sobre equipos informáticos es el examen a distancia del *contenido* de un ordenador (Art. 588 *septies* "a"), ahora bien ¿dicha norma puede ser aplicada a las *comunicaciones* almacenadas en dispositivos, como ser, mensajes de *whatsapp* o correos electrónicos?

La respuesta tiene su importancia dado que la ley de enjuiciamiento criminal española reguló, por un lado, la *interceptación de comunicaciones en tiempo real* (Art. 588 *ter* "a")[53] y, por el otro, el registro remoto y examen de *contenido* de un dispositivo[54].

[53] Artículo 588 ter a. Presupuestos.
La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

[54] Artículo 588 *septies* a. Presupuestos.
1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

El Informe explicativo del Convenio de Budapest indica que por *datos relativos al contenido* "…se entiende el contenido comunicativo de la comunicación, es decir, el significado o finalidad de la comunicación o el mensaje o la información transmitida por la comunicación. Se trata de todo lo transmitido por la comunicación que no sean datos de tráfico"[55], a su vez destaca que su interceptación es una medida muy intrusiva en la vida privada[56].

Y, en especial, con relación al conflicto entre comunicación o dato almacenado el informe explicativo también destaca que "…se plantea la cuestión de si un mensaje de correo electrónico no abierto se encuentra en el buzón de entrada de mensajes de un proveedor de internet hasta que el destinatario lo descargue a sus sistema informático, debe considerarse datos informáticos almacenados, o datos de transferencia. Conforme a las leyes de algunas Partes, ese mensaje de correo electrónico es parte de una comunicación y, por consiguiente, su contenido sólo puede obtenerse aplicando la facultad de interceptación; por el contrario, otros sistemas jurídicos consideran dicho mensaje como datos almacenados a los que corresponde aplicar el artículo 19. Por consiguiente, las Partes deberían analizar su

---

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

[55] Informe explicativo del Convenio sobre la Ciberdelincuencia (STE num. 185), punto. 229. En particular, los datos de tráfico son aquellos datos de la comunicación vinculados al origen, destino, la ruta, hora, fecha, duración, etc.

[56] Informe explicativo del Convenio sobre la Ciberdelincuencia (STE num. 185), punto. 215.

legislación respecto de esta cuestión para determinar lo que es apropiado con arreglo a sus respectivos ordenamientos jurídicos"[57].

Al respecto, Bachmaier Winter plantea con relación a los registros remotos en la legislación española, que "…la alusión al examen del contenido parece implicar que no se contempla la interceptación de comunicaciones en tiempo real. Pero lo cierto es que para las comunicaciones electrónicas escritas esa distinción no tiene mucha relevancia, pues una vez enviadas (abiertas o no, leídas o no), si no se eliminan serán almacenadas en el dispositivo y serían accesibles a través del registro remoto del mismo. En los términos del legislador español, los correos electrónicos almacenados pasan a formar parte del contenido del dispositivo."[58]

Asimismo, la autora destaca que a través de la regulación del registro remoto, la intención del legislador no ha sido abarcar la interceptación en tiempo real de las comunicaciones[59]. Al respecto, interpreto que la autora se refiere específicamente a las comunicaciones en tránsito.

Ello, a mi juicio, es plenamente coherente ya que por el principio de especialidad, la existencia de una regulación más específica como es la de interceptación de comunicaciones en tiempo real (Art. 588 *ter* "a") debería excluir la aplicación del registro remoto (Art. 588 *septies* "a") a esos mismos fines.

En ese orden, se podría acceder al contenido de una comunicación o mensaje por medio de los dos institutos: por el de interceptación de comunicaciones (respecto de los mensajes en tránsito) o por el de registro remoto (mensajes almacenados), sin embargo ambos institutos son distintos y tienen sus particularidades.

Con relación a las diferencias entre ambos, veamos por ejemplo que frente a la interceptación de comunicaciones en tiempo real se presenta un

[57] Informe explicativo del Convenio sobre la Ciberdelincuencia (STE num. 185), punto. 190.
[58] Bachmaier Winter, Lorena, Boletín del Ministerio de Justicia español, LXXI, Nro. 2195, 2017, pág. 14 y sgtes.
[59] Bachmaier Winter, Lorena, Boletín del Ministerio de Justicia español, LXXI, Nro. 2195, 2017, pág. 15 y sgtes.

problema relevante que es la encriptación[60], procedimiento que consiste en el cifrado de los datos informáticos a los fines de favorecer la privacidad de los mismos dificultando la interceptación de terceros. Aplicaciones como *whatsapp* cuentan con el cifrado de los mensajes "punto a punto", es decir, salen cifrados del dispositivo del emisor y sólo se descifran cuando llegan al dispositivo del receptor, sólo puede acceder su usuario a través de la llave criptográfica (la gran mayoría de servicios por internet cifran automáticamente los datos informáticos).

Al respecto, Blanco, con mucha agudeza, destaca que el modelo tradicional de interceptación (Ej.: pinchadura de teléfono) se ve frustrado frente a la encriptación, pues los mensajes en tránsito y de punto a punto se encuentran cifrados; sin embargo, plantea que la forma de soslayar esta dificultad sería la infección del dispositivo en los puntos de entrada o salida para acceder al contenido de los mensajes sin encriptar (pues, se encriptan cuando están en tránsito, no cuando entran o salen del dispositivo del emisor o receptor)[61].

A partir de dicho ejemplo, se puede advertir que si bien la interceptación de comunicaciones puede verse frustrada frente al intento de interceptación en tiempo real, no sería ello así para el instituto del registro remoto, pues este permitiría el acceso al contenido de los mensajes almacenados en el dispositivo del emisor o el receptor.

En razón de lo expuesto, el instituto de la interceptación de comunicaciones es más limitado respecto al del registro remoto que es más intrusivo (ya que este último podría servir para llegar tanto al contenido de un mensaje de *whatsapp* o correo electrónico, como así también a la demás

[60] El cifrado de datos sirve para dar mayor seguridad a las comunicaciones. Cifrar es un procedimiento que utiliza un algoritmo matemático que modifica el contenido del mensaje enviado para dificultar su lectura convirtiéndolo en una secuencia incomprensible de letras, números y símbolos sin sentido. A partir del algoritmo de cifrado, se puede saber que a determinada letra la sustituye otra, a cada símbolo otro, se modificar el contenido del mensaje para saber lo que realmente significa. Muchas aplicaciones tienen cifrados automáticos o cuentan con la posibilidad de aplicarlo a los mensajes. Yubal Fernández. Encriptar: qué es, para qué sirve y cómo cifrar tus archivos (xataka.com). Https:www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos

[61] Blanco, Hernán, Tecnología Informática e investigación criminal, op. cit., pág. 103. Con cita de Bellovin, Steven M. – Blaze, Matt – Clark, Sandy – Landau, Susan, "Going bright: Wiretapping without weakening communications infrastructure", en IEEE Security & Privacy, vol. 11, nro. 1, 2013, págs. 94 y sgtes.

información de la vida privada que un sospechoso pueda tener almacenada en su dispositivo), sin embargo ambos permiten acceder al *contenido* de una comunicación y en este aspecto puntual, es donde deberían equipararse[62] las regulaciones normativas, pues en la regulación española de ambos institutos los delitos de procedencia no son exactamente los mismos, como así tampoco, la duración de las medidas (tres meses prorrogables hasta dieciocho meses –interceptación de comunicaciones, conf. art. 588 *ter* "g"- y un mes prorrogable hasta tres meses –para el registro remoto, conf. art. 588 *septies* "c"-).

§ 8. LOS ACCESOS REMOTOS EN ARGENTINA

a) Su incorporación

En la legislación procesal penal argentina hay pocas normas procesales que regulen institutos destinados a combatir el ciberdelito. Por ejemplo, la provincia de Neuquén ha incorporado los accesos remotos a través de su artículo 153 [63] a su Código Procesal Penal y la provincia de Mendoza tiene un proyecto legislativo en trámite[64], mediante el cual también propone la incorporación de los accesos a su código de procedimiento a través del artículo 216 *ter*[65].

---

[62] Bachmaier Winter, Lorena, Boletín del Ministerio de Justicia español, LXXI, Nro. 2195, 2017, pág. 15 y sgtes.

[63] Artículo 153º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto.
También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota.
A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos.
La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos. (El resaltado dada su importancia).

[64] Expediente de trámite parlamentario Nro.: 0000072000. Link consultado:
https://s3.amazonaws.com/public.diariojudicial.com/documentos/000/084/726/000084726.pdf

[65] "Art. 3º: Incorpórese el artículo 216 ter: "Registro remoto de dispositivos tecnológicos que contengan evidencia digital".
En **supuestos urgentes, tratándose de delitos graves, previstos en los artículos 83, 140, 141, 142, 142 bis, 145, 145 bis, 145 ter, 146, 147 y 170 en el Título III del Código Penal de la Nación, cuando esté en riesgo la vida, la libertad o la integridad sexual de las personas**, si hubiere motivos suficientes para presumir que en determinado dispositivo tecnológico o en un sistema informático, existe evidencia digital pertinente a la
investigación delito, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, ordenará por decreto fundado, bajo pena de nulidad, el registro remoto de ese dispositivo mediante la **instalación de**

El proyecto mendocino identifica expresamente cuáles son los "delitos graves" del Código Penal que habilitan la realización de un registro remoto, como ser: "…supuestos urgentes, tratándose de delitos graves, previstos en los artículos 83, 140, 141, 142, 142 bis, 145, 145 bis, 145 ter, 146, 147 y 170 en el Título III del Código Penal de la Nación, cuando esté en riesgo la vida, la libertad o la integridad sexual de las personas".

Ello, a mi juicio, es un buen punto de partida, ya que la identificación de los respectivos artículos de procedencia disminuye la posibilidad de dudas interpretativas; como podría ocurrir en otro tipo de diseño legislativo, como es el artículo 588 *septies* "a" del procedimiento español, donde la enumeración de delitos de procedencia es sumamente amplia.

No descarto, que como crítica a la técnica legislativa mendocina se puede expresar que la eventual incorporación o modificación de "delitos graves" provocaría la necesidad de modificar el código de procedimiento, no obstante, entiendo que la propuesta mendocina es más respetuosa del debido proceso y derecho de defensa.

Por otro lado, el proyecto mendocino hace expresa referencia "…a la instalación de un *software* que permita el examen a distancia de datos informáticos…", dicha redacción me parece insuficiente, pues limitar su aplicación únicamente a la instalación de un programa malicioso *(software)* deja por fuera otras técnicas o medidas de investigación remota más modernas o las nuevas que puedan aparecer a futuro, como puede ser el ejemplo de Crozono a través de drones (y sin la utilización de un programa tipo *spyware*); en ese orden, considero más acertada la redacción española la cual además de estipular la instalación de un *software*, autoriza "la utilización de datos de

---

un software que permita el examen a distancia de datos informáticos de existencia previa al registro, contenida en el dispositivo tecnológico**.**
La orden debe ser escrita y fundada y deberá especificar: a) Los dispositivos tecnológicos objeto de la medida. b) El alcance de la misma y el software mediante el que se ejecutará el control de la información. c) Los agentes autorizados para la ejecución de la medida. d) Día y hora en que se realizará la medida e) Duración de la medida, que no podrá exceder de un plazo de 48 hs.
Cuando quienes lleven a cabo el registro remoto, tengan motivos suficientes para considerar que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, situado su territorio nacional, podrán ampliar el registro, siempre que los datos sean legítimamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el tribunal, salvo que ya lo hubiera sido en la autorización inicial" (El resaltado dada su importancia).

identificación y códigos"; lo cual permite que la norma a futuro no quede en desuso frente a los constantes cambios tecnológicos.

O, quizás, se podría incorporar en futuros proyectos preceptos más abiertos del tipo: "Técnicas informáticas que permitan la obtención de evidencia digital de manera remota".

Otro punto de interés es que el informe de fundamentos que da origen al proyecto mendocino enumera los diversos tipos de datos informáticos entre los cuales destaca que la "información de contenido" incluye:

1. Contenido (textos y adjuntos) de correos electrónicos que permanezcan en las carpetas de la cuenta (enviados, recibidos, borrador, papelera).

2. Contenido (textos y adjuntos) de los mensajes intercambiados en plataformas de redes sociales.

3. Contenido de publicaciones realizadas en redes sociales cuyo acceso fue restringido al público en general.

4. Historial de localización asociado a la cuenta.

5. Fotos y otros documentos almacenados por el usuario en espacios de alojamiento en la nueve asociados a una cuenta.

Ello, es muy interesante ya que brinda mayor certeza sobre el alcance del registro remoto, véase, por ejemplo, que un correo electrónico almacenado se interpreta como un documento posible de registro por dicho medio informático de investigación (Ver punto 4.2).

Recientemente se ha dado otra modalidad de allanamiento remoto a partir de la provisión al personal policial de un *pendrive* en cuyo contenido se encuentra un software portable (por lo tanto, no necesita ser instalado). El pendrive es montado en el dispositivo identificado como evidencia digital y desde una computadora ubicada en otro lugar un técnico informático accede de

manera remota al contenido del dispositivo a los fines de extraer los elementos que resulten de interés para la investigación[66].

Ahora bien, ¿Cuáles son los límites de dicho procedimiento ejecutado en Córdoba?, ¿Cuál es el sistema regulatorio sobre el cuál se ejecutó la medida?, ¿Es constitucional el ejercicio de una medida tan invasiva?, etc. son algunas de las preguntas que procesalmente aún no tienen respuestas claras y las que intentaré abordar en forma amplia a través del siguiente punto.

b) La libertad probatoria y los límites a la aplicación de institutos no previstos

Sobre la base de lo expuesto hasta aquí, es un importante avance que se haya comenzado a legislar lentamente en algunas provincias argentinas institutos procesales destinados a combatir los ciberdelitos o delitos graves, en especial el registro remoto, pues el alto nivel de intrusión y la grave tensión que se produce por medio de dicho instituto en la intimidad y privacidad (Art. 18 y 19, CN) requieren de una regulación específica y respetuosa de los derechos fundamentales.

Con relación a ello, nuestro más Alto Tribunal al analizar otras medidas de investigación análogamente intrusivas, como la interceptación de comunicaciones telefónicas, ha destacado que "…sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen…"[67].

A mi entender el referido antecedente jurisprudencial excluye toda posibilidad de incorporación en un proceso penal de medios no legislados y tan intrusivos, como puede ser, un acceso remoto. Lo cual, permite limitar interpretaciones amplias del principio de libertad probatoria establecido, por ejemplo, en el Código Procesal Penal Federal conforme a su art. 134, mediante

[66] Https://www.mpfcordoba.gob.ar/novedoso-el-ministerio-publico-fiscal-de-cordoba-realiza-con-exito-allanamientos-en-remoto/.
[67] CSJN, "Halabi, Ernesto c/ PEN – ley 15. Dto.1563/04 s/ amparo ley 16.986", entre otros.

el cual en muchas ocasiones se pretende adaptar forzadamente las investigaciones digitales a los medios de prueba tradicionales (ej.: allanamiento, registro, secuestros, etc.).

Salt, al tratar el tema de la libertad probatoria destaca que es "…necesario distinguir adecuadamente (o individualizar) aquéllos medios probatorios que, aunque novedosos, no significan la aplicación de coerción por parte del Estado o de injerencia en el ámbito de derechos fundaméntales, de aquellos mecanismos de investigación, procedimientos probatorios o medios de prueba que implican una actividad del Estado que por su injerencia en garantías fundamentales de los imputados o de terceros requieren una habilitación legal expresa. En este último supuesto, no resulta posible la aplicación analógica de normas procesales.[68]

Por otro lado, el propio Código Procesal Penal Federal destaca expresamente la protección de los derechos a la intimidad y privacidad de las personas, los que únicamente podrían ser afectados con autorización judicial (Art. 13 de dicho Código), y que como regla de interpretación debe efectuarse una interpretación restrictiva de todas las disposiciones legales que limiten un derecho, prohibiendo la interpretación extensiva y la analógica de dichas normas (Art. 14 del mismo Código).

Sobre la base de dichos artículos, si los accesos remotos no se encuentran regulados no puede prosperar el principio de libertad probatoria para su aplicación, pues, el referido artículo 13 es un primer límite que hace a su inaplicabilidad, ya que: ¿de qué modo, en qué términos, con qué alcance y sobre la base de qué precepto legal debería un juez autorizar la medida de allanamiento remoto? Si por analogía se intentará asimilar dicha medida de investigación informática a un allanamiento tradicional, las diferencias son evidentes, por ejemplo, en lo formal es habitual que los códigos de procedimiento determinen que la orden debe ser notificada al que habite o posea el lugar o encargado, etc. antes de iniciarse el procedimiento [69], esta

[68] Salt, Marcos, Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, op. cit., pág. 47 y sgtes.

[69] Código Procesal Penal Federal. ARTÍCULO 145.- "Formalidades para el allanamiento. La orden de allanamiento **será comunicada entregándose una copia de ella al que habite o posea el lugar donde**

cuestión sería incumplible ya que no tendría sentido efectuar un allanamiento remoto si se le avisará previamente al sospechoso sobre su realización[70].

En las inspecciones de lugares también es común la presencia de dos testigos de procedimiento para que firmen el acta, dicho recaudo tampoco tendría un efecto análogo al que puede ocurrir en un allanamiento tradicional, pues, qué podría declarar un testigo sobre un procedimiento de acceso remoto llevado adelante por un especialista informático a través de medios tecnológicos sofisticados como la instalación de un *malware* en la computadora de un sospechoso o la intrusión en su red de *wi-fi* a través de un dron o la ejecución de pen drive portable conjugado con el uso de una computadora a distancia como en el caso cordobés. La forma de control del procedimiento de medidas informáticas debe ser otra, por ejemplo, las técnicas de *hasheo*.

A su vez, el referido artículo 14 del Código Procesal Penal Federal, a mi juicio, es otro límite importante al principio de la libertad probatoria, dado que la interpretación restrictiva de las normas que limiten un derecho y la prohibición de la interpretación extensiva y analógica de las mismas, son lo que harían inaplicable la extensión de los institutos de prueba tradicionales (ideados para la obtención de evidencias físicas –detectables a través de los sentidos-) a dispositivos tecnológicos (cuyo contenido es informático y compuesto por 1 y 0 –no detectables a través de los sentidos-)[71].

Pérez Barberá sostiene que en un Estado de Derecho debe interpretarse en forma amplia el principio de legalidad penal, tanto para el derecho material como para el derecho procesal, y consecuentemente rechazarse el principio de libertad probatoria por inconstitucional, en un lúcido razonamiento el autor destaca que “La propia formulación del principio de legalidad penal en el art. 18 de la Constitución Nacional muestra su indudable vigencia en materia procesal penal. No ser “penado” sin “juicio” fundado en ley anterior al hecho del

---

deba efectuarse o, cuando esté ausente, a su encargado o, a falta de éste, a cualquier persona mayor de edad que se hallare en el lugar, preferentemente a los familiares del primero. El funcionario a cargo del procedimiento deberá identificarse e invitará al notificado a presenciar el registro. Cuando no se encontrare ninguna persona, ello se hará constar en el acta…”. (El resaltado me pertenece).

[70] Pérez Barberá, Gabriel, “Nuevas tecnologías y libertad probatoria en el proceso penal”, ponencia presentada en el VI Encuentro Nacional de Profesores de Derecho Procesal Penal en Salta, mayo de 2009, pág. 5.

[71] Pérez Barberá, Gabriel, “Nuevas tecnologías y libertad probatoria en el proceso penal”, op. cit., pág. 2 y siguientes.

"proceso" constituye una formulación castellana del *nullum crime, nulla poena sin lege* que coloca en primera línea a la referencia procesal para fijar la extensión del principio". En efecto si de lo que se trata es de no ser penado sin juicio previo, entonces la "ley" a la que hace referencia la formulación constitucional es no sólo la ley penal material, sino también la ley procesal"[72].

El principio de libertad probatoria promueve un campo fértil de acción para que se produzcan posibles desviaciones por parte del Estado, que le permitan inmiscuirse irregularmente en la privacidad y utilizar medios apartados de las leyes para obtener datos, arrojando así "…sombras oscuras en el proceso penal"[73]. Siendo el Estado quien condena "…debería regir el principio de que sólo puede hacer lo que le está expresamente permitido, quedándole prohibido todo lo demás (art. 19, CN). Que esto incluso mejor, se ve en la profusa regulación minuciosa y de detalle que tienen los medios expresos, circunstancia demostrativa de que no es muy normal contar también con medios de prueba fantasmas respecto de los cuales, muy por el contrario y por definición, se sabe poco, quedando todo el formulario de funcionamiento de esas pruebas a rellenar por la jurisprudencia y los usos: inseguridad y contradicción aseguradas"[74].

En ese orden, siendo que la ley debe ser el freno a los actos de los poder estatal, estipular reglas normativas amplias, como el principio de libertad probatoria, que habilitan o abren hacia adentro del poder una zona liberada de arbitrio[75] otorgan un extenso margen de interpretación con remotas consecuencias, limitadas a los diversos puntos de vista y emociones de cada juez en las diversas etapas del proceso[76], cuyo resultado provoca incertidumbre e inseguridad.

Al respecto, parte de la doctrina española se ha expedido sobre la cuestión, planteando que no se puede suplir la necesidad de una *lex scripta, lex stricta y lex praevia*, debiendo contar con una mínima base legal que regule

[72] Pérez Barberá, Gabriel, "Nuevas tecnologías y libertad probatoria en el proceso penal", op. cit., pág. 7.
[73] Clariá Olmedo, Jorge A., Derecho Procesal Penal, Tomo I, Ed. Rubinzal Culzoni 1998, pág. 228.
[74] Pastor, Daniel R., Lineamientos del nuevo Código Procesal Penal de la Nación, Hammurabi, 2015, pág. 78.
[75] García Pullés, Fernando, Lecciones de Derecho Administrativo, Abeledo Perrot, 2015, pág. 36
[76] Beccaria, Cesare, *Dei Delitti e delle Pene (1976)*, Clásicos del Derecho, El Foro, Ciudad Autónoma de Buenos Aires, 2010, pág. 53.

las garantías, requisitos y límites, con normas procesales claras y detalladas "…sin que sea posible una aplicación analógica de la regulación establecida respecto de otras medidas de investigación que pueden guardar cierta relación…"[77], pues en donde hay una regulación legal insuficiente la jurisprudencia puede, en algunos casos, interpretar y adecuar la aplicación de un instituto procesal, pero otra situación muy distinta es donde ni siquiera se encuentra legislada esa realidad, frente a esta situación la jurisprudencia no puede crear lo que no existe legislativamente[78].

En razón de lo expuesto hasta aquí es sumamente importante que se regulen con la mayor celeridad posible reglas claras de procedimiento que permitan investigar adecuadamente delitos graves e informáticos.

§ 9. CONCLUSIÓN

La presente investigación me lleva a concluir que la incorporación de los accesos remotos son una realidad insoslayable en la persecución de delitos graves y cibernéticos, las particularidades de los datos informáticos distan enormemente de los medios de prueba tradicionales, por lo cual la utilización de medidas probatorias desactualizadas y no destinadas especialmente a recolectar evidencia digital no pueden ser aplicados, es necesaria una regulación específica que habilite medidas de investigación específicas destinadas a investigar ciberdelitos.

Los Estados a partir de los *hackeos* legales tienen un poder de intrusión nunca antes visto, deben ser limitados mediante principios procesales claros, estrictos y respetuosos de los derechos fundamentales, como surgen de modernas legislaciones tales como la de España (modificada en el año 2015).

Las investigaciones avanzan vertiginosamente, un claro ejemplo de ello es que los allanamientos remotos hace poco tiempo eran realizados

[77] Ortiz Padillo, Juan Carlos, Estudios de progreso. Fundación Alternativa. La investigación del delito en la era digital. 74/2013, pág. 36

[78] Oubiña Barbolla, Sabela, Cesión de datos personales entre procesos penales y procedimientos sancionadores o tributarios en España y la Unión Europea (Aranzadi), "Datos personales y nuevas diligencias de investigación tecnológica: oportunidades, retos y límites", Aranzadi, 2017, págs. 221 – 277.

exclusivamente mediante *spywares* y actualmente ya pueden ser ejecutados a través de drones o robots, permitiendo así la obtención subrepticia de datos almacenados en un dispositivo electrónico y superando barreras arquitectónicas.

Por lo tanto, la redacción de nuevos proyectos normativos que pretendan la incorporación de accesos remotos deben ser más amplios y no estar limitados únicamente a la utilización o instalación de *software* en el dispositivo electrónico a investigar.

Preceptos legales que establezcan, por ejemplo: “Técnicas informáticas que permitan la obtención de evidencia digital de manera remota” podrían ser más receptivos a los constantes avances tecnológicos que caracterizan a los medios de investigación informáticos.

Sin perjuicio de los constantes avances tanto de la tecnología como de los códigos procesales en diversos países del mundo, Argentina ha incorporado lenta e incipientemente en algunos pocos códigos provinciales los registros remotos, el tema debe ser tomado como una política nacional que sirva para dar coherencia y fundamento a los sistemas procesales de todo el país, mientras tanto los ciudadanos se encuentran al descubierto ante los ciberdelincuentes.

Las leyes procesales argentinas siguen sin estar a la altura de las circunstancias.

BIBLIOGRAFÍA CONSULTADA

- Beccaria, Cesare, *Dei Delitti e delle Pene (1976)*, Clásicos del Derecho, El Foro, Ciudad Autónoma de Buenos Aires, 2010.
- Bachmaier Winter, Lorena, Boletín del Ministerio de Justicia español, LXXI, Nro. 2195, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", 2017.
- Bielli, Gastón Enrique y Ordoñez, Carlos Jonathan, La Prueba Electrónica, La Ley, Ciudad Autónoma de Buenos Aires, 2019.
- Blanco, Hernán, Tecnología Informática e investigación criminal, Ciudad Autónoma de Buenos Aires, La Ley, 2020, pág. 103. Con cita de Bellovin, Steven M. – Blaze, Matt – Clark, Sandy – Landau, Susan, "Going bright: Wiretapping without weakening communications infraestrcuture", en IEEE Security & Privacy, vol. 11, Nro. 1, 2013.
- Clariá Olmedo, Jorge A., Derecho Procesal Penal, Tomo I, Ed. Rubinzal Culzoni 1998.
- Di Orio, Ana Haydée, Info Lab, El rastro digital del delito, 2017.
- García Pullés, Fernando, Lecciones de Derecho Administrativo, Abeledo Perrot, 2015.
- Gris Muniagurria, Pablo H. – Cherñavsky, Nora A. – Moreira, Diógenes A., en Sistema penal e informática, Vol. 2, Phishing: abordaje del fenómeno desde la prevención y la investigación, Ed. Hammurabi, Buenos Aires, 2019.
- Kerr, Orin S., *Executing warrants for digital evidence: the case for use restrictions o non responsive data*.
- Litvin, Jorge Luis, Hackeados. Delitos en el mundo 2.0 y medidas para protegernos, 2020.
- Nilles, Gerardo y Silva, Gastón, Pericias informáticas para casos de pornografía infantil, SID 2016, 16º Simposio Argentino de Informática y Derecho.
- Oubiña Barbolla, Sabela, Cesión de datos personales entre procesos penales y procedimientos sancionadores o tributarios en España y la Unión Europea (Aranzadi), "Datos personales y nuevas diligencias de investigación tecnológica: oportunidades, retos y límites", Aranzadi, 2017.
- Pastor, Daniel R., Lineamientos del nuevo Código Procesal Penal de la Nación, Hammurabi, 2015.
- Pérez Barberá, Gabriel, "Nuevas tecnologías y libertad probatoria en el proceso penal", ponencia presentada en el VI Encuentro Nacional de Profesores de Derecho Procesal Penal en Salta, mayo de 2009.
- Presman, Gustavo Daniel, Cibercrimen II, "La cadena de custodia en la evidencia digital", Editorial BdeF, Buenos Aires, 2018.

- Rodríguez Lainz, José Luis, Sobre la ley orgánica de modificación de la LECRIM para el fortalecimiento de las garantías procesales: la regulación de las medidas de investigación tecnológica.
- Salt, Marcos, Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, Ad-Hoc, Ciudad Autónoma de Buenos Aires, 2017.
- Sergi, Natalia, Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina, Vol. 3, Buenos Aires, pág. 15 y sgtes.
- Taruffo, Michele, La Prueba, Marcial Pons, Madrid, 2008.
- Werner, Braian Matías, Sistema penal e informática, Vol. 2, El allanamiento de dispositivos como un nuevo allanamiento de domicilio en la era digital, 2019.