


# “La evidencia digital en el proceso penal de la provincia de Buenos Aires”

Alumno: Agustín Miguel Eusebio.

Título al que aspira: Abogado.

Tutor: Dr. Hernán Moyano.

Teléfono: 15-5863-4417

Dirección: Roca Nro. 2141 Florida, Vicente López

E-mail: eusebioagustín@hotmail.com

Fecha de entrega: Octubre de 2020

Sede: Centro.

# Mail de reserva y propuesta de tutor

**Solicitud**

De: eusebioagustin@hotmail.com

Para: marilina.miceli@uai.edu.ar

Enviado: jueves, 18 de julio de 2019 04:33 p.m.

Asunto: Tesis

"*Estimada Dra. Miceli:*

*Me dirijo a Ud. A los fines de hacerle saber el tema seleccionado para el trabajo final a presentarse el día 15 de Octubre del corriente año, a saber:*

*"La evidencia digital en el proceso penal."*

*Asimismo pongo en su conocimiento que el presente trabajo ha sido tutorado por el profesor Hernán Moyano.*

*Sin más, la saludo atte.*

*Agustín Eusebio*"

**Respuesta**

De: marilina.miceli@uai.edu.ar

Para: eusebioagustin@hotmail.com

Enviado: jueves, 19 de julio de 2019 10:11 a.m.

Asunto: Tesis

"*Tema reservado. Atte*."

# Agradecimientos

A los docentes con los que he tenido el placer de relacionarme en estos años, durante los cuales me han brindado todo su conocimiento, fueron una pieza imprescindible en mi formación académica.

Al profesor Hernán Moyano, mi tutor, por su gran contribución y paciencia en todo el desarrollo de este trabajo.

A mis compañeros y amigos de clase, durante estos cinco largos años, por hacerlos más felices y por el empuje fundamental que significó su acompañamiento.

A mi familia, mis hermanos, abuelos, tíos, en especial a mis padres por confiar siempre en mí y apoyarme incondicionalmente en todos mis sueños y en todas mis decisiones, en las victorias así como en las frustraciones.

A mis amigos por su aliento, y aguante en todas las reuniones y ocasiones en que no me pude hacer presente.

A Natalia, por su ayuda incalculable y por estar siempre en los momentos que cuentan.

# Resumen

El presente pretende ser una labor investigativa en torno a la utilización de las tecnologías de la comunicación y la información disponibles como herramientas de la persecución criminal. Es mi intención evaluar de qué manera deben ser instrumentadas para convivir en armonía con las garantías constitucionales del debido proceso. El primer problema que se presenta, es que la legislación procesal penal de la provincia de Buenos Aires no ha recogido al momento la noción incipiente de evidencia digital, lo que ocasiona que en la práctica se torne dificultoso incorporar ese tipo de prueba por las particularidades que reviste y a las que haré referencia a lo largo de este trabajo. Me adentraré particularmente en estudiar la posibilidad de implementar el registro remoto de dispositivos electrónicos en el marco de la pesquisa criminal. Analizaré si es necesaria una reforma procesal que incluya esta como otras herramientas digitales, o si resulta inocuo llevarla a cabo en el marco legal de los medios de prueba hoy mencionados expresamente por el plexo normativo aludido.

**Palabras clave:** evidencia digital – proceso penal – herramientas disruptivas de investigación – medios de prueba – principio de libertad probatoria – garantías del debido proceso – registro remoto de dispositivos electrónicos – derecho a la intimidad - secreto de las comunicaciones – protección de datos personales – cibercrimen – derecho informático.

# Objetivos

I)- En primer lugar, hacer una breve introducción al sistema acusatorio que rige el proceso penal de la provincia de Buenos Aires, sus particularidades y los medios de prueba que contempla.

II)- Desarrollar las características propias de la evidencia digital y su diferenciación con la evidencia física.

III)- Estudiar de qué maneras puede implementarse prácticamente el registro remoto de dispositivos electrónicos.

IV)- Establecer pautas objetivas para su implementación.

V)- Analizar la posibilidad de llevarlo a cabo mediante la aplicación análoga de otros medios probatorios reglados como el registro de morada o las intervenciones telefónicas.

VI)- Realizar un relevamiento del derecho comparado.

VII)- Arrimar una posible solución al problema que reviste el atraso legislativo.

## Áreas temáticas a trabajar

El derecho procesal penal, derecho constitucional y derecho informático.

## Técnicas metodológicas

El presente trabajo de investigación científica es de tipo documental y explicativo, no experimental, tal como se puede observar a lo largo del mismo como se fueron utilizando diferentes fuentes bibliográficas tales como textos de derecho, estudios técnicos, normativa tanto nacional como internaciones y diversas publicaciones relacionados con el tema que aquí nos ocupa. Las técnicas empleadas en este estudio son la recolección y análisis de la información, la revisión bibliográfica e internet.

## Hipótesis

Estudiaré en concreto la siguiente hipótesis: Resulta indispensable la implementación de una reforma del Código Procesal Penal de la provincia de Buenos Aires a los fines de introducir la noción de evidencia digital en general y al registro remoto de dispositivos electrónicos como medio de prueba en particular.

# I- Lineamientos generales

## I.I- Introducción del tema y su justificación.

En los tiempos que corren, las tecnologías de la información y la comunicación han empapado por completo la cotidianeidad de los que habitamos esta era. En la actualidad resulta impensado escindir la vida diaria del mundo digital, toda vez que ineludiblemente, muchos de nuestros actos y quehaceres cotidianos se encuentran ligados de alguna manera u otra, al uso de herramientas cibernéticas. Esta nueva realidad, alcanza también al sistema jurídico que nos regula como sujetos sociales.

Si bien es cierto que se han realizado grandes progresos, por definición, el Derecho es contingente. Es creado por el hombre a medida que se van dando cambios en la convivencia del orden social, y necesita de una constante actualización que vaya de la mano con la evolución de la sociedad y con las nuevas maneras de vincularse que ahora nos presentan la época y el momento cultural que transitamos, marcado por la época digital y las tecnologías de las comunicaciones.

Esas nuevas formas de vinculación que menciono, se traducen en el universo del sistema penal en novedosas modalidades delictivas que surgen inevitablemente mucho antes de que puedan ser legisladas como conductas ilícitas. Entre ellas, podemos encontrar al *pishing*, el *pharming*, el *vishing*, el *grooming*, el *ransomware*, etc. sumado a los delitos ya tipificados pero que con los adelantos informáticos adquieren nuevas maneras de comisión (estafas, amenazas, coacción, incluso hasta delitos contra la integridad sexual, etc.), habiendo dado paso al complejo mundo de lo que hoy conocemos como cibercrimen o ciberdelincuencia.

Ahora bien, tal como surgen de manera constante y se multiplican exponencialmente, nuevas maneras de cometer delitos y nuevas figuras delictivas *per se*, sería atinado innovar también en el abordaje de la investigación de esos crímenes, otorgándole a los operadores judiciales, investigadores y profesionales forenses, herramientas legales rápidas y efectivas, procurándose al mismo tiempo que la injerencia estatal se mantenga respetuosa de los derechos y garantías consagradas constitucionalmente.

Encontrar dicho equilibrio, constituye un desafío de gran porte, pues en materia probatoria y como resulta característico de un Estado de Derecho, sólo la prueba lícitamente obtenida e incorporada de igual forma al proceso, es la que puede ser eventualmente valorada para afirmar la materialidad ilícita de un hecho y achacarle la autoría y responsabilidad –en términos penales- del mismo a un sujeto.

En virtud de ello, se hace menester analizar, de qué manera debe colectarse la evidencia digital en el caso de que -como mencioné supra- estemos ante la posible comisión de un delito, sin que ello implique desandar los caminos recorridos en dirección a una administración de justicia más equitativa y respetuosa de las garantías contempladas por nuestro plexo normativo de mayor jerarquía.

Necesariamente, en este trayecto nos toparemos con varias preguntas-problema, a las que intentaré acercar soluciones a lo largo del presente trabajo. Analizaré puntualmente, la obtención de evidencia digital contenida en un dispositivo electrónico, lo que normalmente se realiza mediante el secuestro previo del soporte físico o hardware, en el marco de una requisa o de un allanamiento de un domicilio. Como ejemplo, un Smartphone, un disco rígido externo de almacenamiento de datos, un pendrive, una computadora.

Pero, dado el avance tecnológico, es posible la utilización de un software especial de acceso remoto que no requiera necesariamente que los investigadores y/o forenses se hagan previamente con el objeto que contiene los datos o información, sino que accedan a distancia, optimizando los recursos y acelerando los tiempos de la pesquisa. Como veremos, esta herramienta -como toda disrupción- representa algunos conflictos, dada la sensibilidad y privacidad que caracterizan a esa información personal a la que se alude y a que no existen al momento normas claras y precisas de cómo deben llevarse a cabo un procedimiento de tal índole.

En primera instancia, corresponde, cuanto menos, que nos hagamos las siguientes preguntas: ¿Estamos autorizados a adaptar las normas procesales vigentes a nuestros fines o el derecho de forma escrito es el que necesita *agiornarse* a las nuevas modalidades de investigación posibles? ¿Es factible la aplicación análoga de los instrumentos legislados o es menester hacernos de herramientas superadoras? ¿Cuán urgente es la demanda de una reforma procesal con perspectiva digital?

# II- Breve recorrido histórico por nuestro sistema de enjuiciamiento

## II.I- Justificación de la mención

Previo a adentrarnos en el problema que aquí nos atañe, no resulta caprichoso realizar una sucinta reseña del desarrollo histórico del Derecho Procesal Penal argentino, para entender su evolución y recorrido.

En principio corresponde hacer referencia a que conforme a nuestra organización federal, encontramos divergencias en los sistemas de enjuiciamiento adoptados por las provincias, siendo que como herederos forzosos de la inquisicón europea, todavía sobreviven sus vestigios en algunos ordenamientos, lo cual afortunadamente, tiende a desaparecer.

Por ello, para comprender acabadamente de dónde venimos y hacia dónde vamos, es que considero necesario esta mención a los orígenes de nuestro sistema procesal penal.

## II.II- La inquisición

Durante la última parte de la Edad Media, entraron en conflicto los señoríos feudales con el poder del monarca, quién pretendía aglutinar las diferentes comarcas que reconocía bajo su dominio, sobre la base de una única forma de organización política central. La lucha se decidió a favor del segundo, y el triunfo dio origen a los estados nacionales, cuya idea cultural sigue vigente, y al sistema de organización política llamado absolutismo o monarquía absoluta.

El sistema político se caracterizó por la concentración de todos los atributos de la soberanía -legislar, juzgar y administrar-, en la figura del rey. Correlativamente, el período reflejó un notable crecimiento de la Iglesia Católica. Esta contienda entre el señorío local y el poder central, se tradujo en el avasallamiento del Derecho local nacido de la tradición popular, por parte del Derecho Romano Canónico.

En dicho contexto, se abrió paso el sistema de enjuiciamiento que hoy conocemos como la inquisición, en el siglo XII, aboliéndose el procedimiento acusatorio, se pasó de un debate oral y público, hacia una investigación cumplida por un

inquisidor secreto y por escrito, transformando al acusado de un sujeto, a un objeto de la investigación que se practicaba.[1]

Como características salientes, podemos mencionar a la persecución de oficio, la facultad de los funcionarios de investigar la posible comisión o preparación de un delito por la sola sospecha, incluso basada en un rumor público. La predominancia de la idea del procedimiento como una pura investigación de los hechos por sobre todo vestigio del debate judicial, el triunfo de la escritura por sobre la oralidad, el secreto de la investigación, la prisión como regla en el procedimiento y la defensa como un mecanismo poco influyente en la decisión final.

## II.III- El derecho procesal penal hispanoamericano

Realizando un gran salto cronológico, luego del desarrollo de la inquisición en Europa, con sus marchas y contramarchas, en mérito a la brevedad nos trasladamos hacia el momento en que la conquista y la colonización hispánicas en América trajeron consigo el sistema de persecución penal imperante en Castilla.

El procedimiento penal se rigió por Las Partidas, el cuerpo legal sancionado por Alfonso X, apodado “El Sabio”, promediando el Siglo XIII, que alcanzó una gran difusión en América y determinó el procedimiento común. Permitió así la persecución penal de oficio, la pesquisa oficial escrita y secreta, que admitía también la tortura para descubrir la verdad y la apelación de los fallos en el orden jerárquico establecido para los tribunales creados.[2]

## II.IV- El Iluminismo y la reforma del sistema inquisitivo

En el Siglo XVIII, cobró vital importancia el papel desplegado por los filósofos tales como Motesquieu, Beccaria y Voltaire. A partir de la necesidad de imponer un sistema republicano de gobierno que reemplazar al absolutismo monárquico, y de la dignidad del ser humano, se postuló un nuevo sistema de enjuiciamiento penal, bajo la influencia del Derecho Romano Republicano y el Derecho Inglés, que había resistido el avasallamiento del Derecho romano canónico oportunamente.

---

[1] Maier, Julio B. J., en Derecho Procesal Penal, Tomo I, Fundamentos, Buenos Aires, Ad Hoc, 2016, pg. 273.
[2] Maier, Julio B. J., op. cit., pág. 313.

El nuevo modelo proponía, en lugar de la escritura y el secreto de los procedimientos, de la negación de la defensa y de los jueces delegados del poder imperial, la publicidad y la oralidad de los debates, la libertad de la defensa y el juzgamiento por jurados. Se erigió el debate contra la tortura, como método de averiguación de la verdad. Es decir: comenzó el retorno hacia la acusación popular, sistema propuesto por los modelos republicanos griego y romano de la antigüedad.

Aún así y pese a la sanción del Code d´isntruction criminelle francés de 1808, que dio por terminado a cinco siglos de Inquisición en Europa continental, se dio a luz a un nuevo sistema mixto, que conservó los conceptos de *persecución penal pública* y de la *averiguación objetiva de la verdad histórica*[3] como fin último del proceso, aunque moderados por los novedosos valores individuales referentes a la dignidad humana forjados en la Revolición Francesa. A esta altura, comenzaría la eterna puja entre las injerencias estatales y las garantías fundamentales, inherentes a las personas.

## II.V- La situación en la actualidad

El sistema actual, en palabras de Julio Maier, responde -o al menos así lo intenta- a un Derecho Penal de Acto, (culpabilidad por el hecho) y por ello su meta principal es servir a la reconstrucción histórica del hecho imputado y sus circunstancias de modo, tiempo y lugar, protegiendo la personalidad del presunto infractor.

Se trata de un método reglado con el fin de averiguar la verdad histórica acerca de un hecho humano hipotético que constituye su objeto, método cuyos fines consisten en realizar el poder penal del Estado allí donde él halla fundamento, custodiar la vigencia de los valores superiores relativos a la dignidad de la persona humana y lograr la paz y seguridad jurídicas mediante la decisión final en la que culmina el proceso. [4]

A nivel nacional, y con la sanción del Código de Tomás Jofré, en la provincia de Buenos Aires, en 1915, se introdujo en un intento por modernizar las instituciones procesales de nuestro país, el juicio oral y público para ciertos delitos.

Por otro lado, en 1939 se introduce mediante el Código de Procedimiento Penal de la provincia de Córdoba, una ley de enjuiciamiento moderna, que respeta los postulados mínimos de la carta magna. Constituyó los tribunales de juicio como cuerpos

[3] Maier, Julio B. J., op. cit., pág. 339.
[4] Maier, Julio B. J., op. cit., pág. 354.

colegiados, reguló la instrucción preliminar eminentemente preparatoria, dejando atrás el secreto, salvo para excepciones. Establece fuertemente los principios de inmediación, publicidad, oralidad, etc. Sentó un precedente y un camino a seguir para el resto de las legislaciones provinciales en la materia que le sucedieron.

Actualmente, rige en el Código Procesal de la Provincia de Buenos Aires, la reforma acusatoria vigente desde 1998, momento en el cual el sistema de enjuiciamiento comenzó la transición que aún hoy se considera incompleta, y que ni siquiera saldó la deuda del juicio por jurados previsto constitucionalmente (lo cual recién se contemplaría en el año 2013). Sin perjuicio de ello, en ese mismo momento se sancionaron dos leyes fundamentales para la operatividad del nuevo código, la Ley del Ministerio Público y la Ley de transformación de los juzgados del viejo sistema.

En dicho sentido, todavía no podemos decir que hemos alcanzado satisfactoriamente las exigencias de la Constitución Nacional en materia de administración de justicia penal existiendo aun ciertas reticencias a abandonar por completo el mandato inquisitorial que nos fue legado históricamente.

# III- Las garantías procesales reconocidas constitucionalmente

## III.I- Generalidades

Conforme he desarrollado en el capítulo precedente, el sistema de enjuiciamiento imperante en la actualidad, considera al imputado como un sujeto de derechos y no un objeto de la pesquisa, cuya inocencia debe desvirtuarse, y no al revés.

Es así como las garantías constitucionales, deben entenderse como las seguridades concedidas a los ciudadanos para impedir que el goce de los derechos reconocidos por la Ley Fundamental, sea conculcado por el ejercicio del poder estatal.

En lo que aquí nos ocupa, estos mecanismos resultan de vital importancia, toda vez que actúan como paliativos de la tensión constante entre los derechos fundamentales y la injerencia estatal, en lo que se refiere al ámbito de las investigaciones penales.

Es decir que, el Estado, ante la comisión de un hecho delictivo de acción pública, *debe y puede* investigar, siempre que se produzca la observancia de estas protecciones de las que goza el encausado y que la Carta Magna garantiza.

Existen diversas clasificaciones que engloban estas garantías y las organizan de distinta manera, por lo que aquí me referiré expresamente a aquellas que ponen coto a la actividad probatoria desplegada por los agentes estatales en el marco de una investigación penal.

## III.II- Límites a la actividad probatoria

Ahora bien, como lo he expresado al momento de explicar el recorrido histórico de nuestro sistema procesal penal, y su fuerte antecedente inquisitorial, los límites a la actividad probatoria que se han ido aplicando coinciden en respetar la dignidad del ser humano, impidiendo llevar a cabo el procedimiento penal mediante formas crueles y contrarias al respeto de las libertades individuales.

Es así como la averiguación de la verdad histórica resulta una de las metas a la que está destinado el proceso penal, y las restricciones a la labor de la prueba constituyen algunos de los elementos que se utilizan para evitar que esa meta

desequilibre el sistema invadiendo el ámbito de privacidad e intimidad que garantiza un Estado de Derecho.[5]

A continuación, veremos como dichas limitaciones actúan respecto de la persona del imputado, y de la privacidad y el derecho a la intimidad de las personas.

### III.II.I. Referentes a la persona del imputado

La premisa fundamental que aquí rige, es que él sometido a proceso no puede ser obligado a brindar información, tal como lo establece expresamente el artículo nro. 18 de la Constitución Nacional; "… nadie puede ser obligado a declarar contra sí mismo".

En el mismo sentido, los pactos internacionales de derechos humanos han reconocido también esta garantía, en particular, el Pacto de San José de Costa Rica, en la Convención Americana de Derechos Humanos, art. 8, nro. 2 g; "derecho a no ser obligado a declarar contra sí mismo ni a declararse culpable". Asimismo, lo prevé el Pacto Internacional de Derechos Civiles y Políticos en su art. 14, nro. 3: "Durante el proceso, toda persona acusada de un delito tendrá derecho.. a las siguientes garantías mínimas.. g) no ser obligada a declarar contra sí misma ni a confesarse culpable".

De ello se desprende el carácter de **voluntariedad** que reviste la declaración del imputado, no siendo posible que éste la realice bajo cualquier tipo de coacción, o en contra de su deseo expresado libremente, en cuyo caso no podrá motivar una decisión judicial que lo perjudique.

En ese mismo sentido, la Carta Magna establece que "quedan abolidos para siempre...toda especie de tormento", erradicando la tortura y otros métodos crueles como medio para obtener la verdad.

Aquí cabe aclarar -aunque exceda a los fines de este trabajo- que no sólo representan tortura o utilización de tormentos los apremios de cualquier forma o mediante cualquier instrumento, que provocan un sufrimiento físico, sino también aquellos que provocan un sufrimiento psíquico. Así lo establece la Convención contra la Tortura.

---

[5] Maier, Julio B. J., op. cit., pág. 624.

Tener en cuenta todo ello resulta de suma importancia, porque una declaración brindada por un imputado coaccionado, de cualquier forma que sea, no podrá ser introducida legalmente al proceso, abriendo la posibilidad a que se considere nula, junto con todo lo actuado en consecuencia de ella.

Veremos más adelante como este principio se interrelaciona con algunas otras cuestiones.

### III.II.II. Referentes a la privacidad y al derecho a la intimidad de la persona

Aquí corresponde volver a citar al art. 18 de la Constitución Nacional, el que dispone que "El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación."

De ello, se desprende que, la citada premisa no resulta absoluta, pues el mismo texto constitucional admite que la privacidad que se encuentra protegida, se vulnere **siempre y cuando una ley establezca en qué casos y con qué justificativos** puede traspasarse ese velo de protección.

A diferencia de las prerrogativas analizadas en el punto anterior, siendo claro que nadie podría concebir que una persona sea torturada u obligada a declarar contra sí misma al menos de manera lícita, cierto es que los operadores judiciales sí podrían entrometerse lícitamente en la intimidad de un hogar, o interceptar comunicaciones personales, cuando se respeten las exigencias previstas por una ley preexistente.

Aquí he de destacar que no todas las maneras posibles de injerencia estatal se encuentran debidamente autorizadas por ley, sino que algunas se consideran legítimas de manera análoga. Nos ocuparemos de ello más adelante.

Corresponderá entonces a los ordenamientos procesales provinciales y nacional, regular en qué casos y con qué requisitos es posible introducirse en la esfera de la intimidad de una persona para obtener información sobre la misma y eventualmente introducirla al proceso penal en forma de prueba.

En líneas generales, todos los Códigos de forma exigen para el allanamiento de una morada, la decisión fundada de un juez y su orden escrita, detallando los motivos para presumir que en determinado lugar se encuentran cosas pertenecientes a un delito o está oculto el imputado. También prevén los casos especiales y de urgencia en los cuales excepcionalmente se puede prescindir de la orden judicial escrita.

Exigencias similares rigen para el secuestro de papeles privados y para la interceptación de correspondencia epistolar o telegráfica.[6]

Hasta aquí en rasgos muy amplios, tenemos que el Estado reconoce que las personas gozan de un derecho inviolable, a la intimidad y a la privacidad, que resulta relativo, toda vez que puede ser conculcado si mediaren razones que así lo hiciesen necesario, por ejemplo la sospecha fundada de la posible comisión de un delito de acción pública. Los parámetros para establecer cuándo es debidamente fundada una sospecha, y cuándo no, también han sido materia de debate.

Si hay algo en lo que se ha llegado a un consenso, es que se necesitan motivos previos para que se lleve a cabo la intromisión estatal, pero ¿De qué entidad deben ser esos motivos?, o ¿Cuál es el piso de sospecha mínimo que debe tenerse sobre la existencia de un delito? y ¿Con qué estándares se miden la proporcionalidad, necesidad y urgencia de la medida que se autoriza?.

A modo de marcador del camino, la jurisprudencia ha ido construyendo ciertos parámetros negativos a los fines de justificar o no una injerencia estatal, como por ejemplo al decir la Corte Suprema de Justicia de la Nación, en la causa "Peralta Cano" (P. 1666. XLI) que: "*La mera existencia de una denuncia anónima y la alegación del policía de que uno de los dos jóvenes detenidos llevaba en su mano un destornillador que no fue secuestrado, no son razones suficientes, en este caso, para que nos encontremos dentro de los conceptos de "causa probable", "sospecha razonable" o "razones urgentes"*.[7]

Por su parte, el Código Procesal Penal de la Provincia de Buenos Aires, establece, en su art. 151 que la sola denuncia no basta para proceder a la detención de una persona. Esto es así, porque no podríamos hablar de seguridad jurídica alguna si una simple expresión juramentada bastara por sí para fundar una medida de coerción personal tan delicada como la restricción de la libertad ambulatoria.

Visto ello, y teniendo como plataforma inquebrantable lo establecido por la Constitución Nacional y por la Constitución de la Provincia de Buenos Aires, será

---

[6] Maier, Julio B. J., op. cit., pág. 643.
[7] Escandar Nicolás, y French Santiago en "Injerencias y Estándares Probatorios", Diario DPI Penal N° 93 – 11.12.2015, en línea, consultado el 26/03/2020, disponible en http://www.pensamientopenal.com.ar/system/files/2015/12/doctrina42621.pdf

materia de análisis, cuáles son los tipos de injerencia que están previstos legislativamente, y aun estándolo, causan problemas e interpretaciones diversas.

# IV- El Sistema Probatorio en el Código Procesal Penal de la Provincia de Buenos Aires

## IV.I.- Consideraciones Generales

Retomando el contenido del art. 18 de la Constitución Nacional, según el cual se establece que nadie puede ser penado sin un juicio previo, el que a su vez debe estar fundado en una ley anterior al hecho que origina el proceso. Esto funciona como uno de los límites que se le impone a la actividad probatoria del Estado y es importante aquí aclarar que **la prueba**, es el sustento fundamental de la condena que eventualmente se dicte, así como también de los actos coercitivos jurisdiccionales que pueden dictarse en el marco de un proceso.

Se entiende por prueba toda actividad procesal dirigida a comprobar o descartar la existencia de hechos que guardan relevancia con el objeto del proceso y habiliten a los órganos públicos competentes a adoptar decisiones de mérito, particularmente en lo que se refiere al ejercicio de la reacción penal y procesal penal.[8]

Es así como en el marco de la actividad probatoria, suelen identificarse los conceptos *medio de prueba, objeto de prueba, órgano de prueba y sujeto de prueba*.

El *medio de prueba* es el procedimiento previsto o implícitamente autorizado por la ley tendiente a lograr el ingreso al proceso del material probatorio (Por ejemplo una declaración de un testigo, un peritaje balístico).

El *objeto de prueba* es todo aquello que puede y debe ser probado (Los hechos que se imputan).

El *órgano de prueba* es el sujeto que tiene un elemento de prueba y lo transmite al proceso (ejemplo, el defensor o el representante del Ministerio Público Fiscal).

Y por último el concepto de *sujeto de prueba* hace referencia a las partes que tienen el derecho de ordenar o de proponer la actividad probatoria.[9]

---

[8] Beraldi, Carlos A., en Proceso y Procedimientos Penales de la Provincia de Buenos Aires, coordinadores Pedro J. Bertolino y Alberto. Silvestrini, Buenos Aires, Abeledo Perrot, 2013, pg. 312.
[9] Beraldi, op. cit., pág. 313.

## IV.II.- La libertad probatoria

El art. 209 del Código Procesal Penal de la Provincia de Buenos Aires establece que *"Todos los hechos y circunstancias relacionados con el objeto del proceso pueden ser acreditados por cualquiera de los medios de prueba establecidos en este Código.*

*Además de los medios de prueba establecidos en este Código, se podrán utilizar otros siempre que no supriman garantías constitucionales de las personas o afecten el sistema institucional. Las formas de admisión y producción se adecuarán al medio de prueba que resulte más acorde a los previstos en este Código."*

Dicho ello, tenemos que rige en nuestro sistema, la llamada libertad probatoria, siendo que el plexo normativo autoriza la utilización de otros medios de prueba no previstos expresamente, siempre que no conculquen las garantías constitucionales de las personas.

En lo que respecta a la admisibilidad de la prueba, se pueden dar distintas situaciones según nos encontremos en la investigación preliminar preparatoria o en la etapa del debate.

En el primer caso, se destacan los siguientes supuestos:

Ante la denegatoria del fiscal de producir prueba que se le solicita, la parte interesada podrá requerir que el superior jerárquico de aquél reexamine el pedido luego de dictarse el cierre de la etapa preparatoria y antes de que se formule la requisitoria de apertura a juicio, conforme lo estable el art. 334, párrafo segundo.

Si la medida solicitada tuviera el carácter de irrepetible, y el paso del tiempo la tornase de imposible realización, se podrá solicitar la intervención jurisdiccional.

En el marco del debate, el juicio negativo de admisibilidad es mucho más restringido para el tribunal, sólo facultado para sugerir la prescindencia de aquella prueba que aparezca como manifiestamente impertinente, superabundante o superflua. Así lo determina el art. 338. [10]

[10] Beraldi, op. cit., pág. 315.

## IV. III. La valoración de la prueba

La valoración de la prueba es el examen crítico de los elementos probatorios introducidos en el proceso con el propósito de adoptar alguna decisión de mérito.[11]

Así, la manda procesal se alinea con el llamado sistema de libre convicción o reglas de la sana crítica, el cual exige al juzgador que fundamente y haga explícitos los motivos de la decisión que está tomando.

El art. 210, establece que "*Para la valoración de la prueba sólo se exige la expresión de la convicción sincera sobre la verdad de los hechos juzgados, con desarrollo escrito de las razones que llevan a aquella convicción. Esta regla rige para cualquier etapa o grado de los procedimientos, salvo el caso del juicio por jurados en el que rige la íntima convicción.*"

Vuelvo a destacar que este sistema de valoración no sólo rige al momento de dictar la sentencia, sino para cualquier etapa del proceso.

## IV.IV. Las exclusiones probatorias

Por otro lado, y como contrapeso de la libertad probatoria imperante, el art. 211 del Código provincial establece que *"Carecerá de toda eficacia la actividad probatoria cumplida y la prueba obtenida, con afectación de garantías constitucionales."*

De este modo, tenemos por un lado una suerte de pase libre en materia probatoria otorgado por el digesto procesal, y a su vez, como veremos seguidamente, dedica algunas líneas a establecer parámetros normativos para algunos medios probatorios que selecciona caprichosamente, dejando abierta la posibilidad de que se utilicen de manera análoga y terminando por concluir que el límite común es la afectación a las garantías constitucionales.

## IV.V. Los medios de prueba regulados expresamente

En ese sentido, encontramos que se encuentran referidos expresamente las inspecciones y reconstrucción del hecho, en los arts. 212 a 218, institutos de registro, en

---

[11] Vélez Mariconde, Alfredo, en Derecho Procesal, T. I, Lerner, Buenos Aires, 1968, pg. 351 citado por Beraldi, Carlos A. en op. cit. pág. 315.

el art. 219, el allanamiento de morada, en el art. 220, el de otros locales en el art. 221, el allanamiento sin orden el art. 222, la requisa personal en el art. 225, secuestro en los arts. 226 a 231 bis, la interceptación de correspondencia, en el art. 228, la intervención de comunicaciones telefónicas en el art. 229, etc.

Si bien hemos mencionado muchos de ellos, es mi intención ceñirme en este trabajo al registro domiciliario, la interceptación de correspondencia, y la intervención de comunicaciones telefónicas, aclarando que dicha distinción no resulta huérfana de sentido sino que los mencionados suelen ser los medios utilizados de manera análoga cuando se trata de una investigación desarrollada parcial o totalmente en un medio digital.

**IV.V.I. El registro domiciliario**

El registro domiciliario es un medio de prueba que se encuentra tutelado constitucionalmente por el art. 18, el cual asegura la inviolabilidad del domicilio, es por eso que la diligencia debe observar formalidades especiales determinadas por las legislaciones procesales.

Respecto de la noción de *domicilio*, Badeni sostiene que: *"El concepto constitucional de domicilio tiene un significado considerablemente más amplio que el que emana de la legislación civil. Comprende tanto el hogar como la residencia, el domicilio comercial o cualquier otro espacio físico, móvil o inmóvil, sujeto al uso de una persona y destinado al uso de una actividad privada, pública o semipública*."[12] Teniendo en mira este concepto podemos decir entonces que la protección sobre el domicilio, no es solo sobre el lugar en donde la persona tiene su vivienda, si no que abarcaría ciertos lugares en donde la persona desarrolle un razonable nivel de intimidad. Es decir que domicilio e intimidad, son significaciones que están íntimamente ligados.

Se entiende también por domicilio como todo lugar cerrado o delimitado dentro del cual alguna persona o autoridad tiene un derecho real de posesión, tenencia o cualquier otro que le permita seleccionar o impedir el ingreso de terceros.[13] Por lo cual, se sostiene que si el ingreso es consentido no requiere de orden judicial.

---

[12] Badeni Gregorio, "Tratado de derecho constitucional", La Ley, 2da Ed., 2006, pág. 527.
[13] Beraldi op. cit., pág. 325

En el caso del Código Procesal de la provincia de Buenos Aires, se encuentra reglado por los arts. 219 a 224.

El art. 219 determina que "*Si hubieren motivos para presumir que en determinado lugar existen personas o cosas relacionadas con el delito, a requerimiento del Agente Fiscal, el Juez ordenará, por auto fundado, el registro de ese lugar.*

*El Fiscal podrá disponer de la fuerza pública y proceder personalmente o delegar la diligencia en funcionarios de la Policía. La orden será escrita y contendrá el lugar y el día en que la medida deberá efectuarse, y en sus casos, la habilitación horaria que corresponda y la descripción de las cosas a secuestrar o personas a detener. Asimismo consignará el nombre del comisionado, quien labrará acta conforme a lo dispuesto en los artículos 117 y 118. Esta misma formalidad se observará en su caso y, oportunamente, en los supuestos de las demás diligencias previstas en este capítulo*."

Por su parte, el art. 220 define las reglas del allanamiento de morada; "*Cuando el registro deba efectuarse en un lugar habitado o en sus dependencias cerradas, la diligencia sólo podrá realizarse desde que salga hasta que se ponga el sol.Sin embargo, se podrá proceder a cualquier hora cuando el morador o su representante lo consientan o en los casos sumamente graves y urgentes o cuando peligre el orden público, sin perjuicio de su ratificación posterior por el Juez.*" Entonces, tenemos que la medida tiene que estar dispuesta por el juez a pedido del agente fiscal y por auto fundado; la orden debe ser escrita y detallar el lugar, fecha, horario y las cosas a secuestrar o personas a detener; y por último, deberá consignar el nombre del agente comisionado para el registro, quien dado el carácter de irrepetible del acto deberá documentar lo actuado. Mediante estos recaudos se busca evitar procedimientos arbitrarios y desproporcionados. La obtención de alguna prueba infiriendo alguna garantía constitucional acabará en su eliminación del proceso judicial por pena de nulidad, y en consecuencia no podrá ser utilizado en contra del imputado. A raíz de esto entra en cuestión, una regla derivada de la doctrina conocida como *frutos del árbol envenenado*, esta se va a aplicar cuando ante la obtención ilegitima de

elementos probatorios, los consecuentes que se hayan incorporado de manera correcta también carecerán de validez, porque son frutos de la prueba originalmente viciada.[14]

Antes de continuar, cabe destacar la suma importancia que posee la fundamentación judicial a la hora de emitir un allanamiento en perjuicio de la protección constitucional del domicilio, como sostiene la Corte Suprema de Justicia de la Nación: *"... tal derecho federal solo es realizable de modo efectivo restringiendo ex ante las facultades delos órganos administrativos para penetraren él, sujetando la intromisión a la existencia de una orden judicial previa debidamente fundamentada, exigencia esta última que se deriva del mismo art. 18 de la Constitución Nacional. Solo en ese sentido puede asegurarse que los jueces, como custodios de esa garantía fundamental, constituyen una valla contra el ejercicio arbitrario de la coacción estatal, pues, si su actuación solo se limitara al control ex post, el agravio a la inviolabilidad de este derecho estaría ya consumado de modo susceptible de ser reparado, ya que la Constitución no se restringe a asegurar la reparación sino la inviolabilidad misma."*[15]

Por otra parte, será válido el secuestro de elementos demostrativos de un delito distinto al que genero la orden, siempre y cuando sean aquellos que la policía a través de sus sentidos –jurisprudencialmente conocida como ¨a simple vista¨- encuentre relevantes en comisión de algún tipo de actividad criminal. Esta doctrina fue creada por la Corte de los EEUU, a partir de los casos "Harris vs. United States" de 1968 y "Coolidge vs. Hampshire" de 1971, y es conocida como *plain view doctrine*. Lo que permite la misma, como se mencionó antes, es que la policía en cumplimiento estricto de su cometido, se haya inadvertidamente topado con un elemento constitutivo de un delito distinto a aquel por el que se dispuso la diligencia.

Habiendo descripto las formalidades para la ejecución del registro domiciliario, cabe aclarar que la ley procesal habilita en ciertos casos a la policía, a llevar acabo un allanamiento si previa orden judicial, tal como se especifica en el art. 222, cuando: se denunciare que se ha visto a una persona ingresar a un domicilio con intenciones de cometer un ilícito; durante una persecución el imputado de un delito ingrese en una casa o local; o en caso de que voces provenientes del interior de una morada pidan socorro o

---

[14] Pietro Pastorino Josefina, "Allanamiento y requisa", en "Medios de prueba en el proceso penal", Hamurabi, Volumen 3, 2018, pág. 121 a 152.
[15] CSJN, Fallos 333:1674, 31/08/2010, "Quaranta, José Carlos s/inf ley 23.737".

adviertan que se está cometiendo un delito. A su vez, por motivos de celeridad y con previo aviso al juez de garantías el Art. 19 del código procesal provincial, faculta al fiscal a ordenar directamente el registro de lugares.[16]

**IV.V.II. La interceptación de correspondencia**

Al igual que la anterior, es una medida que se encuentra amparada por la Ley Suprema en su Art. 18, y en el Código Procesal Penal de la Provincia de Buenos Aires en el art. 228, que reza: "*Siempre que se considere útil para la comprobación del delito, el Juez, a requerimiento del Agente Fiscal, podrá ordenar, mediante auto fundado, la interceptación y el secuestro de la correspondencia postal y telegráfica; o de todo otro efecto remitido por el imputado o que se le destinare, aunque sea bajo nombre supuesto. Recibida la correspondencia o los efectos interceptados, el Juez procederá a su apertura, en presencia del Secretario, haciéndolo constar en acta. Examinará los objetos y leerá por sí la correspondencia. Si el contenido tuviere relación con el proceso, ordenará el secuestro; en caso contrario, lo mantendrá en reserva y dispondrá la entrega al destinatario, bajo constancia."*

Mientras que el art. 230 establece la prohibición de interceptar las cartas o documentos que se envíen o entreguen a los defensores para el desempeño de su cargo. La interceptación de correspondencia también deber ser ordenada por un juez, a requerimiento del fiscal, por auto fundado. Consiste en la interrupción o desvió del curso que debe seguir una correspondencia – comprende toda comunicación para la cual se utilice el correo ya sea escrita, paquete, bulto, pliego, valor, etc.-, desde el envió por parte el remitente y la recepción del destinatario, hacia el juez que la ordene. Quien al momento de su recepción procederá, en presencia del secretario, a su apertura y constatación en actas. Examinará los objetos y leerá para sí el contenido, el cual en caso de tener relación con el proceso procederá a su secuestro, caso contrario dispondrá su reserva y posterior envió al destinatario bajo constancia de lo sucedido.[17]

[16] Beraldi, op. cit., pág. 325.
[17] Beraldi, op. cit., pág. 330.

**IV.V.III. La intervención de comunicaciones telefónicas**

En este último caso, estamos ante una medida que a diferencia de las anteriores no existe una cláusula constitucional expresa que la ampare, por lo que su protección resulta análoga, como bien dice el Dr. Bidart Campos se encuentran "…resguardadas por el secreto, como relacionadas con los arts. 19 de la Constitución Nacional (intimidad) y con el 18 (inviolabilidad de correspondencia y papeles privados, por extensión a toda otra comunicación interpersonal, reservada); con el 14 (analógicamente como faz negativa de la expresión libre no destinada a terceros) y como tuteladas en los tratados internacionales de derechos humanos…"[18]. En esta misma línea, la Ley de Inteligencia Nacional 25.520, coloca dentro de esta protección a facsímiles o cualquier otro tipo de sistema de envió de objetos o transmisión de imágenes, datos, voces y todo archivo privado.

A pesar de no estar expresamente amparada constitucionalmente, esta medida deberá cumplir con los mismos requisitos que las anteriores para llevarse a cabo cuando existan motivos que la justifiquen, siendo estos: la orden judicial, a pedido del fiscal y mediante auto fundado.

El Código procesal de la provincia la cristaliza en su art. 229: "El Juez podrá ordenar a pedido del Agente Fiscal, y cuando existan motivos que lo justifiquen y mediante auto fundado, la intervención de comunicaciones telefónicas del imputado y las que realizare por cualquier otro medio, para impedirlas o conocerlas."

El fin de la medida podrá ser, tomar conocimiento de las comunicaciones y su contenido o bien impedirlas, este último caso, si bien es válido, no genera una vía probatoria. Como sucede con la intercepción de correspondencia, en este medio de prueba existen excepciones que no permiten su intervención, como son las comunicaciones amparadas bajo el secreto profesional o la garantía de no ser obligado a declarar contra sí mismo.[19]

Como se observa, nada se dice al respecto de los requisitos para obtener y/o preservar evidencia digital que pudiere contenerse en diversos dispositivos electrónicos,

---

[18] Rocha Degreef Hugo, "El empleo de la interceptación telefónica como medio de prueba", Revista "El derecho", tomo 143, año 1991, pág. 963.
[19] Beraldi, op. cit., pág. 331.

sino que sólo se limita a establecer los reglamentos necesarios para llevar a cabo los medios probatorios clásicos.

Por lo cual, en la práctica veremos que dichos mecanismos sí previstos, serán utilizados de manera análoga a los fines de aplicarlos al mundo digital cuando tengamos delante una investigación que así lo requiera, forzando los moldes previstos por el legislador.

Aquí agrego, deberíamos atender a la distinción que plantea Bruzzone, en cuanto realiza una diferenciación muy valiosa entre *medios de prueba en general*, y *medidas de coerción* a través de las cuales pueden incorporarse elementos de prueba. Esto resulta no menor, ya que en el segundo caso, nos toparemos con afectaciones en mayor o menor medida a garantías consagradas constitucionalmente. En ese andarivel el autor propone que ante la situación de disponerse una medida de prueba que implique coerción, se establezcan pautas objetivas que permitan controlar analíticamente si su utilización es correcta o no.[20]

[20] Bruzzone, Gustavo A., "La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal, en Estudios sobre justicia penal", Editores del Puerto, Buenos Aires, 2005, pág. 248.

# V- La Evidencia Digital

## V.I.- Definición

¿De qué hablamos cuando hablamos de evidencia digital –en términos penales-? ¿Posee características propias? ¿Cuáles son sus diferencias con la evidencia física? ¿Cómo debería ser su tratamiento?

En palabras de Gustavo Raúl Sain, la evidencia digital está representada por los datos e información digital que se almacena, transmite o recibe en un dispositivo electrónico, y puede tener valor para una investigación criminal.[21]

Está construida por campos y pulsos que pueden ser recolectados, almacenados y analizados con herramientas técnicas especiales. He aquí la primera diferencia con la evidencia física: para colectar evidencia digital necesitamos determinados métodos y conocimientos técnicos.

También se observa que posee características que le son propias; la evidencia digital es volátil, intangible, sensible, anónima, duplicable, alterable, modificable y eliminable. Por todo ello, en todas las etapas de la investigación, la misma resulta susceptible de contaminación y/o alteración.

Del mismo modo se ha dicho que su carácter especial se debe a su origen en sí mismo, por tratarse de información que es almacenada en soportes electrónicos, donde su conductor o vehículo es la electricidad, y su traducción se realiza por medio de una interfaz de lenguajes, como el código binario en principio, hasta que aparece representado como texto, imagen, o video, en las pantallas de los dispositivos digitales. Esta información a su vez se encuentra codificada en diversos niveles de lenguaje que van desde el más básico, como el binario y el D.O.S., hasta las más complejas interfaces, que nos permiten disfrutar de los contenidos multimedia sin tener que escribir secuencias de comandos como a principios de la década de los 80 cuando nacieron las primeras PC. Por esto se dice que la prueba digital es intangible, no es corpórea, aunque siempre estará contenida en un medio físico de almacenamiento, como

[21] Sain, Gustavo Raúl, Delito y nuevas tecnologías, fraude, narcotráfico y lavado dedinero por internet, Editores del Puerto, 2012, pp 110, citado por Kiefer, Mariana y Vacarezza, Tomás en Evidencia digital: algunos problemas procesales, Temas de Derecho Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, Tribunales, Volumen 3, Buenos Aires, 2015, pág. 201.

por ejemplo, una computadora de escritorio, o una portátil como las netbooks, notebooks, ultrabooks, tablets, smatphones, tarjetas de memoria, pendrives, discos rígidos extraíbles, soportes ópticos como el CD, DVD, Blu Ray, etc.[22]

Sin perjuicio de ello, la información propiamente dicha, o prueba informática, no es otra cosa que información codificada en diversos lenguajes informáticos alojada en los dispositivos electrónicos, por eso resulta de vital importancia su preservación, el uso correcto de la cadena de custodia, asegurar el material y conocer de manera exacta quién, cómo y cuándo se tomó contacto con el mismo.

Conforme a la "Guía Integral de empleo de la informática forense"[23] de la Procuración General de la Provincia de Buenos Aires, se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de un medio tecnológico informático.

Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. La evidencia digital presenta características que la diferencian de las restantes clases de evidencia física. Se la puede duplicar de manera exacta (permitiendo manipular la réplica sin alterar el original); está sujeta a riesgos específicos de posible alteración y/o eliminación; su localización puede ser muy dificultosa; etc.

Según el documento sobre tratamiento de la Evidencia Digital del Consejo de Europa, las diferencias más destacadas entre la evidencia digital y la física, son:

" **Necesidad de una experticia:** el dato informático no es visible para las personas sin conocimientos y formación técnica especial. Es decir que se requiere de una experticia en la materia, a los fines de aprovechar esa información y al mismo tiempo, para tratarla con el cuidado que requiere y no alterarla.

**Fragilidad y volatibilidad:** El dato informático es muy frágil y volátil. En algunos casos, las pruebas electrónicas están almacenadas en dispositivos electrónicos

---

[22] Sueiro, Carlos Christia, en "La prueba digital en la criminalidad informática: a propósito del nuevo Código Procesal Penal", en Ledesma, Angela, E.; dir, "El debido poceso penal: doctrina. Análisis jurisprudencial. Fallos fundamentales", Hammurabi, Volumen I, Buenos Aires, 2016, pág. 122.

[23] Guía Integral de Empleo de la Informática Forense en el Proceso Penal, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, en línea, consultado el 02/02/2020, disponible en http://www.pensamientopenal.com.ar/system/files/2019/02/doctrina47360.pdf.

en los que cualquier acción puede alterar su estado. El cambio en la memoria de los dispositivos puede ocurrir por alterar el estado original en el que se encontró un equipo (por ejemplo, apagarlo o encenderlo) lo que genera la necesidad de mecanismos especiales para asegurar la cadena de custodia de los datos.

**Peligro de alteración:** El contenido original puede ser alterado o destruido incluso mediante el uso habitual del dispositivo electrónico. El estado de la memoria de los dispositivos electrónicos cambia constantemente, ya sea por voluntad del usuario ("guardar documento", "copiar archivo") o bien automáticamente por el sistema operativo ("asignar espacio para programa", "almacenamiento temporal de datos para intercambio entre dispositivos").

**Grandes extensiones de información:** La masividad de la información digital y dificultad para la búsqueda de la información pertinente para el objeto procesal. La capacidad creciente de almacenamiento de los dispositivos y el bajo costo económico que significa está generando un número cada vez mayor de documentos digitales. Sin perjuicio de las herramientas informáticas que permiten automatizar los procesos de búsqueda, la identificación de la evidencia digital pertinente en un dispositivo o sistema informático que puede transportar millones de documentos constituye un desafío logístico para los investigadores y un desafío para las garantías individuales por la posibilidad de encuentros causales (o no tan casuales) de información indiscriminada muchas veces alejada del objeto de prueba que habilitó una medida.

**Clonación ilimitada:** La evidencia digital puede copiarse sin límites, en realidad, si la operación se efectúa correctamente y con los instrumentos necesarios no se trata propiamente de copias sino de una clonación ya que los nuevos resultados mantendrían todas las características del original. El contenido electrónico puede copiarse infinitas veces y ser exactamente igual al contenido original. Este atributo único permite realizar múltiples copias exactas al contenido original para ser distribuidas y analizadas por diversos especialistas al mismo tiempo (por ejemplo, puede entregarse una copia bit a bit a la defensa para que realice su propia pericia). De

esta manera una correcta obtención de la prueba digital permite que todas las medidas sean siempre actos de prueba reproducibles, en términos procesales.”.[24]

Por todo ello, el empleo y la manipulación de la evidencia digital en los procesos judiciales -especialmente en los casos penales- presenta complejos problemas jurídicos, vinculados con el derecho a la intimidad y al secreto de las comunicaciones, las posibles afectaciones a terceras personas, etc.

Valga aclarar nuevamente que la evidencia digital no será excluyente de los procesos iniciados en base a la investigación de delitos netamente informáticos, sino que hoy en día, en la era de la hiperconectividad, donde muchas de nuestras actividades cotidianas ocurren o tienen incidencia en el entorno digital, es posible y quizás hasta imperante que los operados de justicia se hagan de prueba informática para llevar adelante cualquier tipo de pesquisa, desde la más simple a la más compleja.

Así las cosas, es menester establecer parámetros para que la prueba pueda ser prolijamente incorporada al proceso, previniendo futuras exclusiones, o cuestionamientos de legalidad. Es decir, es importante hablar sobre la **trazabilidad** de esa prueba, de cara al juicio oral. De la misma manera en que la prueba física debe ser obtenida respetando derechos y garantías, y no es posible utilizarla sin limitaciones.

## V.II. La regulación normativa de la evidencia digital

En nuestro país se encuentra vigente la Ley Nro. 26.388, sancionada el día 4 de junio de 2008, y promulgada el 24 de junio del mismo año, que fue publicada en el Boletín Oficial el día 25 de junio de 2008.[25]

No obstante ello, la citada norma, que resulta modificatoria del Código Penal, no fue concebida como una reforma en materia procesal sino sustantiva, atendiendo parcialmente a los lineamientos de la Convención sobre la Ciberdelincuencia de

---

[24] Sergi Natalia, “Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina”, en Informe realizado para la Asociación por los Derechos Civiles, consultado el 02/02/2020 en línea, disponible en https://adc.org.ar/wp-content/uploads/2019/06/038-analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina-vol-3-04-2018.pdf

[25] Boletín Oficial de la República Argentina, miércoles 25 de junio de 2008, año CXVI, nro. 31.433. Ley 26.388, Código Penal de la Nación Argentina, sancionada el 4 de junio de 2008, promulgada el 24 de junio de 2008 y publicada el 25 de junio de 2008.

Budapest, del 23 de noviembre de 2001, la cual recomienda que los países miembro adapten su legislación procesal al contenido del instrumento internacional.

## V.III- La convención sobre la Ciberdelincuencia de Budapest

El 23 de noviembre de 2001, en la ciudad de Budapest, Hungría, se firmó el instrumento internacional llamado Convention on Cybercrime of the Council of Europe (CETS No.185), conocido en español como Convenio sobre la Ciberdelincuencia de Budapest, con motivo de la celebración de la Conferencia Internacional sobre la Ciberdelincuencia, tratándose del primer estándar internacional creado en la temática.

El Convenio y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión el 8 de noviembre de 2001 y entró en vigor el día 1° de julio de 2004. Fue ratificado al momento por más de 60 países de todo el mundo, pudiendo nombrar regionalmente a Perú, Chile, Brasil. Por nuestra parte, Argentina adhirió el 5 de junio de 2018, habiendo entrado en vigor el día 1/10/2018.[26]

### V.III.I. Antecedentes del Convenio sobre ciberdelincuencia de Budapest

Conforme a su informe explicativo, el trabajo previo a la firma del Convenio, se originó por la decisión CDPC/103/211196, mediante la cual el Comité europeo para los problemas criminales (CDPC) decidió en noviembre de 1996 establecer un comité de expertos encargado de los delitos informáticos.

El CDPC basó su decisión en la siguiente razón fundamental:

"*Los rápidos desarrollos en el campo de la tecnología de la información influyen directamente sobre todos los sectores de la sociedad moderna. La integración de los sistemas de telecomunicaciones y de información, que posibilitan el almacenamiento y la transmisión de todo tipo de comunicaciones, sin tener en cuenta la distancia, crea una amplia gama de nuevas posibilidades. Estos desarrollos se vieron*

[26] Charts of Signatures and Ratifications of Treaty 185 Convention on Cybercrime, en línea consultado el 31/08/2020, disponible en https://www.coe.int/en/web/conventions/fulllist//conventions/treaty/185/signatures?p_auth=5mmNWA6v

*potenciados por la aparición de las redes y las superautopistas de la información, incluida Internet, a través de las cuales prácticamente todas las personas pueden tener acceso a cualquier servicio de información electrónica, sin importar en qué lugar del mundo se encuentre. Al conectarse con los servicios de comunicaciones y de información, los usuarios crean una especie de espacio común, denominado "ciberespacio", que es utilizado con fines legítimos, pero que también puede ser objeto de un uso impropio. Estos "delitos cometidos en el ciberespacio" abarcan tanto actividades que atentan contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones como el uso de esas redes o sus servicios para cometer delitos tradicionales. El carácter transfronterizo de dichos delitos, por ej., cuando se cometen a través de Internet, está en conflicto con la territorialidad de las autoridades nacionales encargadas de imponer el cumplimiento de las leyes. Por consiguiente, el derecho penal debe mantenerse al corriente de estos desarrollos tecnológicos que ofrecen oportunidades muy sofisticadas para hacer un mal uso de las facilidades del ciberespacio y perjudicar intereses legítimos. Dada la naturaleza transfronteriza de las redes de información, es necesario un esfuerzo internacional concertado para hacer frente a ese uso impropio. Si bien la Recomendación núm (89) 9 llevó a cierto grado de aproximación de los conceptos nacionales con respecto a ciertas formas de usos impropios de la informática, únicamente un instrumento internacional de carácter vinculante puede asegurar la eficacia necesaria en la lucha contra estos nuevos fenómenos. En el marco de dicho instrumento, además de las medidas de cooperación internacional, se deberían abordar las cuestiones de derecho sustantivo y procesal, así como cuestiones que están estrechamente relacionadas con el uso de la tecnología de la información."*

Por otra parte, el CDPC tuvo en cuenta el Informe preparado, atendiendo a su pedido, por el profesor H.W.K. Kaspersen, que llegaba a la conclusión de que *"... habría que buscar otro instrumento jurídico más obligatorio que una recomendación, tal como un convenio. Dicho convenio no debería abordar tanto las cuestiones de derecho penal sustantivo como las cuestiones de derecho procesal penal, así como también los acuerdos y procedimientos del derecho penal internacional".*[27] Se había

[27] Aplicación de la Recomendación núm. R (89) 9 sobre delitos informáticos, Informe preparado por el Profesor Dr. H.W.K. Kaspersen (doc. CDPC (97) 5 y PC-CY (97) 5, página 106).

llegado a una conclusión similar en el informe adjunto a la Recomendación núm. R (89) 9[28], concerniente al derecho sustantivo, y la Recomendación núm. R (95) 13[29], relativa a los problemas de derecho procesal en relación con la tecnología de la información.

**V.III.II. Finalidades y conformación del Convenio**

Por el mismo rumbo, el informe explicativo enuncia que el Convenio tiene como finalidad primordial:

1) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos;

2) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico,

3) establecer un régimen rápido y eficaz de cooperación internacional.

En consecuencia, el Convenio tiene cuatro capítulos: I) Terminología, II) Medidas que deberán adoptarse a nivel nacional – el derecho penal sustantivo y el derecho procesal, (III) Cooperación internacional y (IV) Cláusulas finales.

La Sección 1 del Capítulo II (Derecho penal sustantivo) abarca las disposiciones relativas a los delitos y otras disposiciones conexas referentes al ámbito de los delitos informáticos o los delitos relacionados con el empleo de ordenadores. En primer lugar, define 9 delitos agrupados en 4 categorías diferentes y más tarde versa sobre las responsabilidades y sanciones conexas. El Convenio define los siguientes delitos: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

La sección 2 (Derecho procesal) del capítulo II, cuyo alcance va más allá de los delitos definidos en la Sección 1, ya que se aplica a cualquier delito cometido por medio de un sistema informático o a las pruebas que se encuentren en formato electrónico.

---

[28] *La delincuencia informática*, Informe del Comité Europeo para los Problemas Criminales, página 86.
[29] *Los Problemas del derecho procesal penal relacionados con la tecnología de la información*, Recomendación núm. R (95) 13, principio núm. 17.

Determina en primer lugar las condiciones y salvaguardias comunes aplicables a todos las facultades procesales contenidas en ese Capítulo.

A continuación, establece los siguientes poderes procesales: **conservación rápida de datos informáticos almacenados; conservación y revelación parcial rápidas de los datos relativos al tráfico; la orden de presentación; el registro y la confiscación de datos informáticos almacenados; la obtención en tiempo real de datos relativos al tráfico, y la interceptación de datos relativos al contenido**. La última sección del Capítulo II incluye disposiciones en materia de jurisdicción.

El capítulo III contiene las disposiciones relativas a la asistencia mutua en relación con los delitos tradicionales y con los delitos relacionados con la informática, así como también las referentes a la extradición. Da cuenta de la asistencia mutua tradicional en dos situaciones: cuando entre las partes no existen fundamentos jurídicos (tratados, leyes de reciprocidad, etc.), en cuyo caso corresponde aplicar sus disposiciones, y cuando existe dicha base, en cuyo caso los acuerdos existentes también se aplican a la asistencia que se concede en virtud del presente Convenio.

La asistencia específica en materia de delitos informáticos o de delitos relacionados con la informática se aplica a ambas situaciones y abarca, sujeto a condiciones adicionales, la misma serie de facultades procesales definidas en el Capítulo II. Por otra parte, el Capítulo III contiene una disposición acerca de un tipo específico de acceso transfronterizo a datos informáticos almacenados, que no requiere la asistencia mutua (cuando media un consentimiento o cuando están disponibles públicamente) y prevé el establecimiento de una red que funcione las 24 horas del día los 7 días de la semana con el fin de asegurar una asistencia rápida entre las Partes.

Por último, el Capítulo IV contiene las disposiciones finales, las cuales, con ciertas excepciones, recogen las disposiciones habituales de los tratados del Consejo de Europa.[30]

### V.III.III- Terminología del Convenio

[30] Informe explicativo de la Convención de Budapest, en línea, consultado el 31/08/2020 en https://rm.coe.int/16802fa403#:~:text=I.,Conferencia%20Internacional%20sobre%20la%20ciberdelincuencia.

Del mismo modo que el aludido informe explicativo realiza un recorrido por los antecedentes, la finalidad y el contenido del Convenio, en su parte pertinente arroja luz respecto de los términos empleados, como por ejemplo, define un “Sistema Informatico” como “*un dispositivo que consta de hardware y software cuya función es el tratamiento automatizado de datos digitales. Puede incluir facilidades de entrada (input), salida (output) y almacenamiento. Puede funcionar en forma independiente o estar conectado a una red con otros dispositivos similares. "Automatizado" significa sin intervención directa de un ser humano; "tratamiento de datos” significa que los datos que se encuentran en un sistema informático son operados mediante la ejecución de un programa informático. Un "programa informático" es un conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar el resultado deseado. Un equipo puede ejecutar diversos programas. Un sistema informático por lo general consta de diferentes dispositivos, diferenciándose entre el procesador o unidad de procesamiento central y los periféricos. Un "periférico" es un dispositivo que realiza ciertas funciones específicas interactuando con la unidad de procesamiento, como puede ser una impresora, una pantalla de video, un dispositivo para leer o escribir CD u otros dispositivos de almacenamiento de datos. Una red es una interconexión entre dos o más sistemas informáticos. Las conexiones pueden ser terrestres (por ej., alámbricas o por cable), inalámbricas (por ej., radioeléctricas, infrarrojas o satelitales), o de ambos tipos. Una red puede estar limitada geográficamente a un área pequeña (redes de área local) o puede abarcar un área extensa (redes de área extensa), y esas redes pueden a su vez estar interconectadas. Internet es una red global que consta de muchas redes interconectadas que utilizan protocolos comunes. Existen también otros tipos de redes, estén o no conectadas a Internet, capaces de transmitir datos informáticos entre sistemas informáticos. Los sistemas informáticos pueden estar conectados a la red como nodos o pueden ser un instrumento para brindar asistencia en la comunicación a través de la red. Lo esencial es el intercambio de datos a través de la red.*”

Hace lo propio también respecto del concepto de “**Datos informáticos**”, explicando que su definición “*se basa en la definición de datos de la ISO. Esta definición contiene las palabras "que se preste a tratamiento informático". Esto significa que los datos están en un formato tal que pueden ser procesados directamente por un sistema informático. Con el fin de aclarar que en el presente Convenio el término “datos” debe entenderse como datos en formato electrónico u otro formato que*

*se preste a tratamiento informático directamente, se introduce el concepto de "datos informáticos". Los datos informáticos que se procesan automáticamente pueden ser objeto de uno de los delitos definidos en el presente Convenio, así como el objeto de la solicitud de una de las medidas de investigación definidas en el presente Convenio*."

Y también, respecto de los llamados "**Datos de tráfico**", "*los "datos relativos al tráfico" tal como se definen en el Artículo 1, acápite d), constituyen una categoría separada de datos informáticos que está sujeto a un régimen jurídico específico. Estos datos son generados por los ordenadores en la cadena de comunicación con el fin de encaminar una comunicación desde su punto de origen hasta su destino. Por tanto, son datos auxiliares a la comunicación misma. En el caso de la investigación de un delito penal cometido en relación con un sistema informático, los datos relativos al tráfico son necesarios para rastrear el origen de una comunicación como punto de partida para reunir otras pruebas, o como parte de las pruebas del delito. Los datos relativos al tráfico podrían tener sólo una duración efímera, lo que hace necesario ordenar su rápida conservación. En consecuencia, su rápida revelación puede ser necesaria para averiguar la ruta de una comunicación, a fin de obtener otras pruebas antes de que sean eliminadas o para identificar a un sospechoso. Por lo tanto, el procedimiento ordinario para la obtención y revelación de los datos informáticos podría ser insuficiente. Además, la obtención de estos datos se considera, en principio, menos intrusiva ya que, como tal, no revela el contenido de la comunicación, que es considerado más sensible. La definición enumera de forma exhaustiva las categorías de datos relativos al tráfico que están comprendidos bajo un régimen específico en el presente Convenio: el origen de una comunicación, su destino, la ruta, la hora (GMT), la fecha, el tamaño, la duración y el tipo de servicio subyacente. No todas esas categorías estarán siempre disponibles técnicamente, o podrán ser suministradas por un proveedor de servicios, o serán necesarias para una investigación penal en particular. El "origen" se refiere a un número de teléfono, dirección de Protocolo de Internet (IP), o a una identificación similar de una instalación de comunicaciones a la que un proveedor de servicios presta sus servicios. El "destino" se refiere a una indicación comparable de una instalación de comunicaciones a las que se transmiten las comunicaciones. El término "tipo de servicio subyacente" se refiere al tipo de servicio que está siendo utilizado en la red, por ej., transferencia de archivos, correo electrónico o envío de mensajes instantáneos. La definición deja a las legislaturas de*

*cada país la posibilidad de introducir algún grado de diferenciación respecto de la protección legal de los datos relativos al tráfico de acuerdo con su sensibilidad. En este contexto, el Artículo 15 obliga a las Partes a establecer las condiciones y salvaguardias adecuadas para la protección de los derechos y las libertades humanas. Esto implica, entre otras cosas, que los criterios sustantivos y los procedimientos que corresponda aplicar conforme a una facultad de investigación pueden variar de acuerdo con la sensibilidad de los datos.*"

**V.III.IV. Medidas procesales recomendadas por la Convención**

El punto 1 del art. 14 de este Convenio establece que: *"...Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos...*".[31]. Podemos decir entonces que a los estados parte no tienen límites ni obligaciones en cuanto a las facultades o procedimientos que pueden establecer con el fin de facilitar la investigación penal de los delitos mencionados anteriormente. No obstante pasaré a desarrollar algunas de las medidas procesales mencionadas y descriptas por el instrumento en cuestión que deberían adoptarse a nivel nacional, asegurando que se mantengan sujetas a las condiciones y salvaguardas previstas en su derecho interno, garantizando una protección adecuada de los derechos y libertades de sus ciudadanos.

El Convenio adapta las medidas procesales tradicionales al nuevo entorno tecnológico. Así escomo en su art. 19 se refiere expresamente al **registro y confiscación de datos informáticos almacenados**:

"1. *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:*

*a) A un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y*

---

[31]Convenio de Budapest, en línea, consultado el 31/08/2020, disponible en https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

*b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio.*

*2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.*

*3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:*

*a) Confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;*

*b) realizar y conservar una copia de dichos datos informáticos;*

*c) preservar la integridad de los datos informáticos almacenados de que se trate;*

*d) hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.*

*4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2."*

Del mismo modo se refiere a la **orden de presentación** en su art. 18; "*Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:*

*a) a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y*

*b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte*

*que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.*

*A los efectos del presente artículo, por* ***«datos relativos a los abonados»*** *se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:*

*a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;*

*b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;*

*c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios."*

Además, propone la creación de nuevas medidas, tales como la **conservación rápida de datos informáticos almacenados** (art. 16) **y sobre el tráfico** (art. 17), con el fin de garantizar que las medidas tradicionales para obtener información, seguirán siendo eficaces en el volátil entorno tecnológico.

Art. 16 de la Convención;

"*1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.*

*2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades*

*competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables…*"

Esta medida consiste en ordenar al encargado o titular de un sistema informático (sea persona física o jurídica, privada o pública) que determinados datos queden preservados mediante mecanismos informáticos por un tiempo determinado sin posibilidad de que sean borrados o alterados. Ello evita el borrado automático de datos por parte del sistema informático en el que los datos están alojados que es de práctica corriente, por costos económicos.[32]

Como los datos en el nuevo entorno tecnológico no siempre son estáticos, sino que pueden estar en movimiento en el proceso de comunicación, se han adaptado otros procedimientos tradicionales de obtención de información pertinentes para las telecomunicaciones, tales como **la obtención en tiempo real de los datos relativos al tráfico** (art. 20) y la **interceptación de los datos relativos al contenido** (art. 21), con el fin de permitir la obtención en tiempo real de los datos electrónicos de tráfico y de contenido, asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático, independientemente de la cantidad de proveedores de servicio que se encuentren involucrados. Siendo, estos últimos, pasibles de ser identificados y la vía por medio de la cual se transmitió la comunicación, con el fin de prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar la transmisión de datos.

Todas las disposiciones contempladas en Sección de las normas procesales tienen como finalidad permitir la obtención o la obtención de datos a los fines de llevar a cabo investigaciones o procedimientos penales específicos. Quienes redactaron el presente Convenio debatieron si éste debería imponer a los proveedores de servicios la obligación de obtener los datos relativos al tráfico y de conservarlos por un período de tiempo determinado, pero finalmente no se incluyó ninguna obligación de esa índole debido a la falta de consenso.

En cuanto a la nueva terminología que surge de esta revolución tecnológica delictiva, y junto con ello estos nuevos medios probatorios podemos decir que, si bien con la intención de reflejar la evolución de los conceptos se introdujeron nuevos

---

[32] Sergi, Natalia, op. cit.

términos como “acceder” y “copiar” más orientados al lenguaje tecnológico e informático, se adoptó un enfoque más flexible, permitiendo que los estados opten por mantener las raíces tradicionales del derecho penal, utilizando conceptos como "registro y confiscación", como así las nuevas nociones de "acceso y copia". [33]

Por último la "autoridad competente" para ordenar, autorizar o llevar a cabo la ejecución de algunas de las medidas procesales mencionadas, u otras diferentes creadas por algún estado parte con el fin de obtener o presentar pruebas en relación con investigaciones o procedimientos penales sobre delitos informáticos, será el que se encuentre facultado por la legislación interna de cada país, ya sea judicial, administrativo o de otra índole.

## V.IV- El contexto normativo en Latinoamérica

Como podremos ver, algunos países de la región se encuentran paulatinamente adaptando sus normas procesales a los medios de investigación tecnológicos y a las particularidades de la evidencia digital, lo que no implica que quede por delante un largo recorrido hacia normativas procesales a la altura de los avances de la época.

A modo de ejemplo podemos nombrar a Colombia que modificó su código procesal penal (Ley 906 del 2004), previendo la Orden de Presentación en su art. 236; y el Registro y Confiscación de datos informáticos almacenados, art. 236 y 244. Por su parte Chile tiene previsto en su código procesal penal el registro y confiscación de correspondencia electrónica, art. 217 y 218. Panamá, en el Código Judicial tiene previsto el registro y confiscación de datos informáticos almacenados (art. 2178), obtención en tiempo real de datos sobre el tráfico (art. 16 de la Ley 16/2004), y la interceptación de Datos sobre el Contenido (art. 16 la Ley 16/2004). República Dominicana en su Ley sobre Crímenes y Delitos de Alta Tecnología (53-07) tiene prevista la conservación rápida de datos informáticos almacenados (art. 54(b)), conservación y revelación parcial rápidas de datos sobre el tráfico (art. 56), orden de presentación (art. 54(a)), registro y confiscación (art. 54(b), (e), (f) y (j)), obtención en tiempo real de datos sobre el tráfico (art. 54(k), e (i)) y obtención en tiempo real de datos sobre el contenido (art. 54(l)). Costa Rica, tiene previsto el registro y confiscación

[33] Informe explicativo de la convención de Budapest, op. cit.

en los artículos 198 y 199 del código procesal penal y artículo 1 de la ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones y la interceptación de datos sobre el contenido: artículo 9 de la ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones. [34]

## V.V- Protocolo para la preservación, obtención y análisis de la evidencia digital de la provincia de Buenos Aires

Como tenemos visto, al momento no contamos con legislación procesal a nivel local que regule la obtención e incorporación al proceso de la evidencia digital, a pesar de que como expliqué oportunamente, impera el principio de libertad probatoria. Por ello, la adquisición, obtención, preservación, peritaje y conservación de la evidencia digital, se realiza aplicando análogamente los preceptos de los medios de prueba física reglados.

Ahora bien, como tenemos visto, la evidencia digital ostenta ciertas particularidades, y en razón de ello, es que deben observarse las maneras correctas de obtenerla, analizarla y preservarla, a los fines de ser introducida al proceso de manera oponible legalmente.

Para subsanar la falta de regulación, existen protocolos dirigidos a los operadores y auxiliares de la justicia, que intentan establecer un orden en las prácticas.

En la provincia de Buenos Aires, se encuentra aprobada mediante Resolución Nro. 483/2016 de la Procuración General, la "*Guía Integral de empleo de la Informática Forense*" basada en el Proceso Unificado de la Recuperación de Información (PURI), cuya adopción en casos concretos permite guiar la actuación informático-forense.[35]

En el marco de lo previsto en el Convenio 5/14 de Investigación y Desarrollo en Informática Forense, suscripto el 29 de mayo de 2014 por la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, la Universidad FASTA y la Municipalidad de General Pueyrredón, se integró el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense y se acordó el desarrollo del proyecto

---

[34] Sergi, Natalia, op cit.

[35] Guía Integral de Empleo de la Informática Forense en el Proceso Penal, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, en línea, consultado el 02/02/2020, disponible en http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1

Protocolo de Actuación en Informática Forense (PAIF) a partir del Proceso Unificado de Recuperación de Información (PURI) oportunamente desarrollado por el Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA el cual tuvo como objetivo el desarrollo de un Protocolo de Actuación en Informática Forense para ser adoptado y promovido por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo. [36]

La Guía Integral de Empleo de la Informática Forense en el Proceso Penal fue finalizada en mayo de 2015, implantada a modo de prueba piloto en los departamentos judiciales de Mar del Plata y Mercedes durante los meses de noviembre de 2015 a marzo de 2016, mediante Resolución Nro. 483/16 de la Procuración General de la Provincia de Buenos Aires y su principal objetivo consistió en establecer una guía de las tareas a desarrollar para la prestación de un servicio forense, ya sea en un ámbito judicial o privado.

Aquí es dable destacar que ante la ausencia de regulación específica y de líneas jurisprudenciales firmes sobre las cuestiones vinculadas con la evidencia digital en el ámbito nacional, se ha tenido especialmente en cuenta la normativa constitucional y los aportes provenientes del derecho comparado. Por esto mismo, la guía integral y el protocolo en particular, pueden representar un estándar válido para modelos procesales similares al bonaerense, adaptable a diferentes modelos de procedimiento, incluso extranjeros, constituyendo un aporte sin precedentes y sumamente valioso para el sistema procesal penal en general.

Las primeras versiones del PURI aspiraron a la definición de un proceso unificado como un “conjunto de fases sucesivas”, que permiten dividir el problema, entender el propósito de cada fase, sus particularidades y la interconexión de las mismas con un todo. Asimismo, cada fase incluye un conjunto de actividades y tareas a realizar con una secuencia lógica, pudiendo las mismas diferir de acuerdo al objeto origen.

El modelo PURI es un esquema teórico de las tareas involucradas en la aplicación forense de las ciencias de la información. Este esquema agrupa las tareas en actividades de mayor abstracción y a estas últimas en fases. A su vez, el modelo se

[36] Guía Integral de Empleo de la Informática Forense en el Proceso Penal op. cit.

complementa con las técnicas para llevar a cabo cada una de esas tareas y las herramientas disponibles para ejecutar dichas técnicas. [37]

En este instrumento se presentan los aspectos básicos a considerar en las labores de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales en el proceso penal, a fin de garantizar la validez y eficacia probatoria de dichas actividades. PURI se nutre de procesos y guías de buenas prácticas en informática forense nacionales e internacionales, adaptándolas e integrándolas en un esquema de fases, etapas, tareas, técnicas y herramientas recomendadas. Se contemplan, de este modo, la planificación previa, la identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva.

Lo relativo a los equipos de telefonía celular es objeto de tratamiento genérico, sin formularse mayores precisiones respecto de las específicas técnicas y herramientas de análisis pericial. Esta última cuestión está siendo objeto de otro proyecto de investigación y desarrollo. Este protocolo debe ser cumplido por los especialistas e idóneos informáticos (en sus distintos niveles y roles), ya que refleja consensos técnicos en la materia y ofrece suficiente respaldo jurídico para su labor. Fiscales e investigadores judiciales deben conocer adecuadamente el protocolo. El mismo es, por un lado, una herramienta para planificar y controlar el curso de una investigación penal. Por el otro, poder invocar su observancia otorga un importante sustento para la presentación eficaz de evidencias digitales y dictámenes periciales durante la labor de litigación. Para desarrollar las tareas informático-forenses y utilizarlas procesalmente es imprescindible alinear la dimensión técnica con sus aspectos jurídico, estratégico y organizacional. Por tal motivo, el protocolo sólo podrá ser aplicado e invocado en forma eficiente teniendo debidamente en cuenta las nociones y recomendaciones generales que obran en el anexo IV (“Aspectos Legales y Estratégicos del Empleo de la Informática Forense en el Proceso Penal”).

Se establecen cuatro principios y características esenciales que debe poseer la evidencia digital: relevancia, suficiencia, validez legal y confiabilidad.

---

[37] Di Iorio, Ana Haydeé y otros, “Buenas prácticas en la extracción y tratamiento de la evidencia digital”, Hammurabi, Volumen 2, Buenos Aires, pg. 212

El primero de ellos actúa como criterio de selección, el especialista que lleva a cargo la investigación debería ponderar la *relevancia* de cierta evidencia en el plan de la investigación o en su defecto dar su opinión a quien la dirija. Este principio tiende a que la evidencia no sea superflua o sobreabundante si no por el contrario pertinente al caso, y suficiente para demostrar lo que se ha investigado o en su defecto convencer a un jurado de aquello, esto último representa el principio de *suficiencia*.

El siguiente es el de *validez legal,* el cual como bien lo indica su nombre tiende a que a la evidencia digital obtenida sea admisible, respetando las garantías, formas legales y reglamentarias consagradas, en caso de injerir derechos fundamentales deberá ser obtenida por orden previa de un juez o de quien dirija la investigación.

Por último, tenemos la *confiabilidad* de la evidencia digital, esta refiere no solo a la aptitud de probar lo que se pretende probar con ella, sino también a como fue obtenida, preservada, analizada y presentada ante el tribunal, este proceso de manejo debe ser justificable, auditable, repetible y reproducible:

Justificable: se va a poder justificar demostrando que los métodos y acciones utilizados son los idóneos, o si otro especialista valida y verifica lo actuado.

Auditable: todas las acciones llevadas a cabo deberán ser documentadas y pasibles de revisión y evaluación por otro experto externo.

Repetible: realizando los mismos procedimientos documentados, respetando las herramientas utilizadas, condiciones y el momento, cualquier especialista tiene que poder arribar al mismo resultado que el original.

Reproducible: como la regla anterior pero con herramientas distintas, en condiciones distintas, en cualquier momento.

Para cumplir con estas reglas, se debe minimizar el manejo de la evidencia original, en caso de ser necesario lo tendrá que hacer un especialista competente, justificándolo y quien será responsable de cualquier modificación. De producirse una alteración irreversible en la misma se deberá informar de ello previamente, y todo lo relacionado a su manejo, o alteración debe estar documentado

Esta actividad que van a desarrollar los técnicos forenses, cumpliendo con los principios mencionados *ut supra,* en relación a la evidencia digital cuanta de seis faces:

“1. Identificación de los equipos, dispositivos y todo otro tipo de medio de almacenamiento cuya obtención y/o examen se considere pertinente y útil para una investigación penal.

2. Recolección de equipos, dispositivos y medios de almacenamiento.

3. Adquisición de datos volátiles. Se trata de la obtención de datos existentes en dispositivos encendidos que pueden perderse definitivamente al ser apagado el artefacto.

4. Cadena de custodia. Por cuestiones de índole práctica, se la trata como proceso de trabajo separado, pese a que suele atravesar varias de las otras fases.

5. Adquisición de medios de almacenamiento persistentes. Esta fase comprende toda actividad vinculada con la generación de una o más réplicas exactas de todo el contenido digital alojado en un dispositivo de almacenamiento persistente (ej. discos rígidos, tarjetas de memoria extraíble, dispositivos USB, tarjetas SIM, entre otros). Su finalidad es la de asegurar la confiabilidad de la evidencia digital, ya sea que se la considere en sí misma o como insumo para la labor pericial o la prueba testimonial. Las réplicas o copias forenses permiten trabajar a los peritos sin alterar la evidencia original.

6. Labores periciales. Las tareas periciales se encomiendan a Especialistas en Evidencia Digital (EED). Las condiciones habilitantes para el ejercicio del rol pericial informático están reguladas en los arts. 2° y 7° inc. 13 de la ley 13.016 de Ejercicio de las Profesiones en Ciencias Informáticas. En cuanto al tipo de labor encomendada, ésta puede consistir en examinar la evidencia y elaborar un informe, o bien en pronunciarse acerca del dictamen de otro perito (ver art. 249 del CPP).”[38]

[38] Guía Integral de Empleo de la Informática Forense en el Proceso Penal, op. cit.

# VI- El registro remoto de dispositivos electrónicos.

Como he adelantado en la introducción a este trabajo, los progresos provistos por las tecnologías de la información y las comunicaciones, hoy hacen posible que no se requiera de manera excluyente del secuestro del soporte físico que contiene la evidencia digital como fuera habitual, sino que es factible el uso de *softwares* especiales para su obtención de manera remota sin el conocimiento del usuario que está sospechado de la comisión de un delito.

En la práctica se solicita al juez que expida una orden de registro domiciliario o allanamiento en la residencia del sospechoso a los fines de proceder al secuestro del o los dispositivos electrónicos que se encuentren bajo la esfera de su custodia. Luego y en un segundo momento, estos dispositivos deberán ser sometidos a tareas de extracción y análisis forense de la información allí contenida (tal como se ejemplifica el protocolo al que me referí en el capítulo anterior).

Orin Kerr, quién brega por la sanción de normas específicas que regulen las investigaciones, se ha encargado de diferenciar estos dos pasos teniendo en cuenta que se tratan de momentos distintos que requieren de órdenes distintas para ser llevados a cabo; en primer lugar, la orden habilitante para ingresar a la morada y secuestrar los dispositivos y en segundo término, la orden que faculte al investigador a examinar el dispositivo secuestrado. Entiende que ocurren dos requisas, en lugar de una; la física y luego la digital. Se pregunta si la "propiedad" a ser registrada debería aludir al soporte físico o a la evidencia digital obtenida durante la búsqueda electrónica y si el "lugar" donde se lleva a cabo la diligencia debería asimilarse al lugar donde se encuentra el *hardware*, el *hardware* mismo o el lugar donde se llevará a cabo la búsqueda electrónica. Del mismo modo encuentra dificultades respecto de en qué lapso de tiempo debe ser llevada a cabo dicha búsqueda, qué tipo de requerimientos deben exigirse para guardar la información y cuándo deben ser devueltos los dispositivos.[39]

En ese sentido advierte Kerr que recabar evidencia digital requiere experticia técnica y un monto considerable de tiempo (vale recordar que la masividad es una de las características de la prueba electrónica y quizás estemos ante la presencia de cantidades

[39] Kerr, Orin Serch, "Warrants in an Era of Digital Evidence", The George Washington University Law School, Public Law and Legal Theory Working Paper Nro. 128, 2005.

monstruosas de información) puesto que luego del secuestro del dispositivo, se requiere una segunda búsqueda dentro del mismo, con el objeto de analizar la información y seleccionar la que resulta relevante para la investigación. Por ello esta segunda búsqueda probablemente sea imposible de llevarse a cabo *in situ*.

Aquí debo hacer referencia expresa a la palabra del experto en la materia, ingeniero Gustavo Presman, quién elaboró en su carácter de perito informático un trabajo de relevamiento sobre el estado actual de la investigación forense digital en América Latina para la Asociación por los Derechos Civiles (ADC). Manifiesta el especialista, que "*en la etapa de recolección de la evidencia digital, debemos distinguir la recolección mediante imágenes forenses y el secuestro directo de los dispositivos. En el primer caso se realiza una copia bloque a bloque del contenido digital almacenado, el que es autenticado mediante una función de HASH para asegurar la integridad de la prueba recolectada. Las imágenes pueden obtenerse a través de un programa o un duplicador forense. Si se utiliza un programa, hay que tener cuidado en impedir la contaminación de la prueba, mediante un acceso al dispositivo que bloquee la escritura o empleando un sistema operativo que no escriba sobre el medio digital. Si se usa un duplicador forense, ya es implícito el bloqueo contra escritura y la velocidad del proceso mejora drásticamente, pudiendo producir múltiples copias. Asimismo, está la técnica del Triage, que permite la recolección de prueba digital mediante el uso de criterios superficiales, a fin de identificar potenciales elementos relevantes para la investigación. En todos estos casos, lo importante es contar con hardware y software especializado y, sobre todo, un insumo fundamental como lo son los discos rígidos necesarios para el almacenamiento de la evidencia recolectada. A pesar de que la regla es evitar acceder al contenido de los dispositivos que contienen evidencia digital para evitar su contaminación, existen ciertas ocasiones en donde el peligro de vida o perjuicio en la demora requiera acceder al dispositivo en vivo. En estos casos, se debe solicitar autorización previa al juez y el perito debe ser muy cuidadoso en los recaudos a tomar en el procedimiento -en especial, su documentación- y circunscribirse sólo a aquellos aspectos de la investigación que han sido ordenados. En el segundo caso, el secuestro de dispositivos, los elementos confiscados deben ser embalados y etiquetados de manera que se resguarde el contenido y sea identificable con claridad. En el caso de los teléfonos celulares, deben*

*ser embalados en contenedores especiales que bloqueen la interferencia electromagnética a fin de evitar que puedan ser accedidos durante el procedimiento*."[40]

Sumado a lo anterior, tengamos en cuenta que hoy en día los dispositivos electrónicos poseen un sinfín de información sobre nosotros y nuestras actividades, -desde fotografías, preferencias políticas y/o religiosas, hasta nuestra geolocalización- por eso es una posibilidad que el investigador o forense se tope tanto con datos relevantes como con otros que no lo sean, incluso podemos hasta imaginar el escenario de un hallazgo accidental de evidencia respecto de un delito distinto al objeto de la pesquisa. Aquí entraría en juego la doctrina del *plain view*, a la que he hecho referencia anteriormente.

Como vemos, esta fragmentación obligada del registro reviste más inconvenientes, dadas las características que como he mencionado *ut supra*, le corresponden a la evidencia digital. Recordemos que la misma se distingue por ser volátil, frágil, fácilmente alterable y masiva. Por esto, imaginemos la situación en la que se realiza una diligencia de allanamiento de una morada, en la que nos encontramos con varios dispositivos de almacenamiento electrónico bajo la esfera de custodia del imputado. Por ejemplo, una Tablet, una computadora de escritorio, una notebook, un Smartphone. La práctica común indica que luego de ingresar y proceder al secuestro de dichos elementos, los mismos serán trasladados al laboratorio forense a los fines de que se comience el proceso de extracción de los datos. Pero, puede suceder también que nos encontremos no con uno, ni con dos, ni con cinco soportes físicos, sino que se trate de por ejemplo varios servers, cuyo traslado se torne dificultoso. O incluso aún, ¿qué pasa si el hecho de trasladar los dispositivos desde la finca hasta el lugar donde serán analizados implica perder de vista al imputado y que el mismo pueda alterar la evidencia mediante el acceso remoto a la nube? Y ¿qué sucede si el investigador desconoce la ubicación física exacta del dispositivo y el acceso remoto aparece como única alternativa? Es así como la necesidad de acceder a distancia a los datos de un imputado puede motivarse en distintos supuestos y el registro remoto pareciera brindar

---

[40] Presman, Gustavo en "La Investigación forense informática en América Latina", compilado por Eduardo Ferreyra para la Asociación por los Derechos Civiles, año 2018, en línea, consultado el 10/02/2020 disponible en https://adc.org.ar/wp-content/uploads/2019/06/037-la-investigacion-forense-informatica-en-america-latina-vol-2-04-2018.pdf.

una solución a estos problemas, existiendo en la actualidad los avances suficientes como para acceder a la información sin siquiera tener contacto físico con el *hardware*. De este modo es posible contar con *softwares* espías o *spywares* capaces de interceptar en tiempo real y grabar datos transmitidos o recibidos a través de diferentes medios de comunicación electrónica, pudiendo incluirse tanto datos de contenido como datos de tráfico de comunicación, hasta datos de geolocalización que nos permita acceder a la ubicación geográfica del dispositivo y por lo tanto del imputado.[41]

Esta herramienta que permite acceder remotamente a un dispositivo que contenga evidencia digital nos abre la posibilidad de sortear los obstáculos que supone la diligencia en dos pasos a la que hace referencia Kerr, y lo más importante aún, nos permitiría llevar a cabo el registro de una manera secreta y asegurarnos el éxito de la investigación.

Aquí entra en escena el siguiente debate: ¿podría brindase al registro remoto de dispositivos el tratamiento de las intervenciones telefónicas de manera análoga? ¿y el de una interceptación de correspondencia? ¿qué similitudes guarda con el registro domiciliario? Sin duda alguna, si en algo se interrelacionan todos estos institutos, es que todos configuran injerencias que ponen en jaque la afectación a garantías de guarda constitucional, como el derecho a la intimidad. Pero incluso, y sólo valiéndonos del sentido común, podemos afirmar con cierto grado de certeza que la afectación a la privacidad resulta sensiblemente mayor cuando tenemos acceso a un dispositivo de almacenamiento informático que cuando ingresamos a un domicilio o realizamos una escucha telefónica. Sin lugar a dudas, lo primero resulta por demás invasivo.

En relación a ello, y como señalé oportunamente (punto IV.IV.III del presente trabajo), resulta valioso atender a la diferenciación que plantea Bruzzone respecto de los medios de prueba y las *medidas de coerción* a través de las cuales se incorpora prueba al proceso, entendiendo en este caso que estamos ante el segundo supuesto por existir afectación a garantías fundamentales y por lo tanto cobra importancia vital establecer parámetros objetivos a los fines de establecer su procedencia.

Al respecto, vale traer a colación la TST 342/2013 de la Sala Segunda en lo Penal del Tribunal Supremo español: "*La ponderación judicial de las razones que*

---

[41] Sergi, Natalia, op. cit.

*justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital. Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías.*"

Del mismo modo, la Sala Segunda del Tribunal Constitucional Español, en la sentencia 173/2011 ha dicho que "*si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) -por lo que sus funciones*

*podrían equipararse a los de una agenda electrónica-, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal ( art. 18.1 CE ), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información.*"

## VI.I. Métodos mediante los cuales puede llevarse a cabo la medida

El acceso remoto a equipos informáticos puede llevarse a cabo fundamentalmente de dos maneras:

1) accediendo a los datos mediante de una red que sea accesible a través del equipo que se ha localizado e intervenido físicamente, bien sea como consecuencia de una entrada y registro o de otra manera;

2) mediante el acceso a los datos almacenados en equipos informáticos que no están físicamente localizados o accesibles, pero a los cuales puede accederse a través de

la utilización de programas espía o *spyware*, un *software* específico que permite acceder en el equipo, sin que su usuario lo advierta.

La primera medida suele denominarse registro ampliado o *extended search of computers*, y la segunda registro remoto o *remote search of computers*. A través del registro remoto mediante el uso de un *spyware*, se podría a su vez acceder a otros equipos que estuvieran conectados a la red del equipo intervenido. El registro ampliado deriva bien del registro directo de un dispositivo de almacenamiento –que está conectado en red a otros equipos– o bien de un registro remoto a través de programas espía, por lo que siempre estará vinculado a alguna de esas dos medidas.[42]

Cuando hablamos de *malware*, o programa malicioso, podemos definirlo como "*cualquier programa informático capaz de ocasionar un daño, ya no sólo al sistema informático en el que se ejecuta, sino al propio usuario, como, por ejemplo, mediante la obtención de sus datos bancarios, de información personal, de archivos íntimos, etc. El malware es un concepto más amplio que el virus informático; abarca también programas como los troyanos, el spyware, los keyloggers, etc."*[43]

Entonces tenemos que el mecanismo funciona de la siguiente manera: el investigador es capaz de valerse de un *malware* espía que ingrese clandestinamente al dispositivo que será el objetivo de la intervención, y hacerse con los datos que sean necesarios, sin que el usuario tome conocimiento de la medida, lo que lo hace una herramienta sumamente poderosa, puesto que se tendrá registro en vivo de los movimientos digitales del encausado, y seguramente por un tiempo prolongado.

Por medio de los procesos informáticos llevados a cabo por estos programas se consigue el llamado *remote search* o registro remoto de equipos. Estos procesos se han definido como "*la técnica consistente en el acceso y registro de los equipos*

---

[42] Bachmaier Winter, Lorena, Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Organica 13/2015, en línea, consultado el 10/02/2020b en https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428206148?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1701_Estudio.pdf&blobheadervalue2=1288794492107.

[43] Amerigo Sanchez J.L., "El régimen jurídico del malware según la Ley de Propiedad Intelectual" Nº 8436, Diario La Ley, 2014, Pág.4 citado por Jorge Sanmartín, Sara, en El uso de virus espía como diligencia de investigación: análisis crítico y propuesta, año 2016, en línea, consultado el 12/02/2020 en https://gredos.usal.es/bitstream/handle/10366/132691/TFM_JorgeSanMartin_Uso.pdf;jsessionid=D46D7727385CF1585F29F9CE906B386F?sequence=1

*electrónicos e informáticos del sujeto investigado, de forma remota y telemática, mediante la previa instalación en el mismo del software necesario -los denominados «programas troyanos»- que permita a las autoridades responsables de la investigación, escanear su disco duro y demás unidades de almacenamiento y remitir de una manera remota y automatizada el contenido del mismo a otro equipo informático (el de la autoridad responsable de la investigación).*"[44]

Precisamente es el llamado virus troyano, caballo de Troya o *trojan horse* uno de los instrumentos más utilizados por cuerpos de investigación debido a las importantes utilidades que supone su uso. La técnica de los troyanos espías consiste en: "*la entrada subrepticia de un programa en el ordenador de un sospechoso, pretende adquirir pruebas y vigilar la actividad de éste, consiguiendo sin su conocimiento, pero con autorización judicial, los datos que aquel almacena en su disco duro o en la memoria del PC, así como toda la actividad comunicativa que no sale a la Red […] además del tráfico de entrada y salida de sus telecomunicaciones y de las páginas web que visita*"[45] .

Otra de las técnicas empleadas para la investigación de delitos mediante diligencias tecnologías es el uso de *keylogger*, o en castellano, lector de teclados. Velasco Nuñez explica que este procedimiento se emplea "*ante la necesidad de captar actuaciones interactivas no monitorizables en el investigado (especialmente su clave y contraseña) pudiera instalarse con autorización judicial como complemento técnico de lo que jurídicamente es la interceptación de la información de interés para la investigación en los ordenadores".*[46]

Respecto de las maneras en que pueden alojarse los *malwares* en los equipos que pretenden intervenirse, existe dos. Una de ellas es instalar ciertos enlaces portadores del mismo en páginas web cuyo contenido sea sospechoso de atraer a determinados delincuentes como pueden ser por ejemplo sitios que se encarguen de distribuir imágenes de abuso sexual infantil. De este modo el usuario estaría auto instalándose el virus al clickear en el botón de descarga. El segundo se interrelaciona con la figura de

---

[44] Ortiz Padillo, J.C., "El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito" ,nº 1, Editorial LA LEY, 2012, Pág. 5 citado por Jorge Sanmartín, Sara, Op. Cit.

[45] Velasco Núñez Eloy, "ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal" Nº 82, Editorial LA LEY, 2011, citado por Jorge Sanmartín Sara, Op. cit.

[46] Velasco Núñez, Op. cit.

agente encubierto informático. [47] Los investigadores envían directamente correo electrónico a los sospechosos conteniendo el enlace malicioso portador del troyano, el que se alojará en el dispositivo y les permitirá hacerse con los datos buscados.

## VI.II. Pautas objetivas a tener en cuenta para su aplicación

En primer lugar hay que tener en claro que el acceso remoto a dispositivos electrónicos mediante el uso de un *malware* espía resulta una injerencia en la esfera de la intimidad personal, como ha quedado de manifiesto, mucho más invasiva que un simple allanamiento de morada o una interceptación de algún tipo de comunicación. Estamos ante un ***nuevo nivel de intimidad o privacidad***, que incluso supera a todos los demás ámbitos de reserva hasta ahora conocidos. Ello, atento a la multiplicidad y sensibilidad de los datos con los que el investigador puede toparse al ingresar al entorno digital privado de una persona. [48]

Asimismo, habrá que analizar en cada caso concreto si la intromisión estatal se encuentra debidamente justificada como para conculcar la protección que la normativa vigente le otorga al derecho a la intimidad, al secreto de las comunicaciones y a los datos personales. Respecto de la protección de estos últimos vale agregar la existencia de la ley de protección de datos personales según la cual se considera que son "*datos personales*" la "*información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*" mientras que son "*datos sensibles*" los "*datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual."*[49]

En este sentido puede afirmarse que resulta una *medida que implica coerción*, para la cual excluyentemente se necesitará el aval jurisdiccional, con la expresión

---

[47] En nuestro país la figura del agente encubierto está prevista por el art. 3 de la ley 27.319, no así la del agente encubierto digital, lo cual abre otra próspera línea de debate cuyo tratamiento escapa a este trabajo. http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.htm#:~:text=ART%C3%8DCULO%203%C2%BA%20%E2%80%94%20Ser%C3%A1%20considerado%20agente,identificar%20o%20detener%20a%20los

[48] En el mismo sentido se manifiesta Marcos Salt en su tesis doctoral citada por SERGI, Natalia, al hablar de que un mayor potencial de intromisión por parte de las herramientas informáticas debiera implicar una mayor protección.

[49] Ley Nro. 25.326 de protección de datos personales disponible en línea en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

fundada de las razones que lo motiven y la que a mi criterio deberá implementarse sólo cuando no existan medios menos lesivos de la intimidad para obtener el resultado deseado, o cuando se encuentre en juego un bien jurídico de mayor jerarquía como la vida o integridad física de las personas. Establecido ello, no será menos importante que lo anterior, exigir proporcionalidad entre la injerencia y el fin que se persigue. Reviste importancia también, exigir un límite temporal a la medida, por su naturaleza de intromisión.

En suma no podemos desconocer que el método resulta tan valioso como intrusivo y también debe tenerse en miras que la búsqueda deberá estar ceñida al objeto procesal previamente determinado y para el cual se ha autorizado la diligencia, haciendo la salvedad de que pudieren ocurrir hallazgos involuntarios de otras evidencias, cuya validez será objeto de una discusión ulterior.

## VI.III. El registro remoto de dispositivos en el derecho comparado

El proyecto HIPCAR denominado "Por una mayor competitividad en el Caribe a través de la armonización de las políticas de TIC, Legislación y Procedimientos Regulatorios" fue lanzado en diciembre de 2008 por la Unión Internacional de Telecomunicaciones (UIT) y la Unión Europea y contó también con la colaboración de CARICOM Secretaría de la Comunidad del Caribe y la Unión de Telecomunicaciones del Caribe (CTU). Incluyó entre sus actividades la elaboración de recomendaciones para una legislación modelo sobre la ciberdelincuencia, modelo normativo que incluye tanto normas de derecho penal de fondo como de proceso penal tendente a la obtención de evidencia digital. Prevé la utilización de técnicas de *remote forensic* como herramientas de investigación. Incluso en su Sección 27, sugiere a los países la adopción de una norma a nivel nacional que prevea estas técnicas de investigación previendo la excepcionalidad de la medida y un uso restrictivo atendiendo a la potencialidad de afectación a la intimidad que significa su uso.[50]

En España, la medida de acceso remoto a sistemas informáticos fue incorporada con una reforma legislativa surgida, de acuerdo al texto de la exposición de motivos, de la necesidad de modificar aspectos de la Ley de Enjuiciamiento que no pueden esperar

[50] Sergi, Natalia, Op. Cit.

la reforma integral que está aún en proceso de discusión. Resulta ser la Ley Orgánica 13/2015, del 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación pretende regular en el campo de las diligencias de investigación tecnologías. Las medidas que recoge el texto legal se engloban desde el capítulo IV en adelante y son las siguientes: la interceptación de las comunicaciones telefónicas y telemáticas (capítulo V), la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos (capítulo VI), la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (capítulo VII), el registro de dispositivos de almacenamiento masivo de información (capítulo VIII) y registros remotos sobre equipos informáticos (capítulo IX).

El registro de dispositivos de almacenamiento masivo de información se encuentra acogido por el art. 588 septíes b de la mencionada Ley de Enjuiciamiento;

*"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.*

*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.*"

En Alemania fue más complicada esta implantación pues su Tribunal Supremo había declarado que no existía norma legal en la que poder amparar el uso del acceso remoto como diligencia de investigación. Fue necesario un cambio de planteamiento por parte del Tribunal Constitucional Alemán (Bundesverfassungsgericht) 36y el reconocimiento por parte de este de un nuevo derecho fundamental (el "Derecho Fundamental a la garantía de la confidencialidad e integridad de los equipos informáticos") para reformar la Bundeskriminalamt (Ley del Servicio Federal de Investigación Criminal) e incluir esta posibilidad.[51]

En lo que respecta a nuestro país, en el año 2017 fue presentado en el Senado nacional un proyecto de ley de reforma del Código Procesal Penal de la Nación, en el que se pretendía incluir a la evidencia digital y a los medios de prueba tecnológicos, incluso, el art. 235 bis del proyecto se refirió al registro remoto, al expresar que *"También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota"* sin brindar mayores precisiones ni pautas de implementación.[52]

El antecedente inmediato de ello resulta el proyecto de actualización del Código Procesal Penal de la Nación en materia de Informática Jurídica y Criminalística Digital, realizado en el marco del programa "Justicia 2020", del año 2016, [53] donde se planteó la

---

[51] Sanmartín Jorge, Op. Cit.

[52] Proyecto 3010/17 en línea, consultado el 10/08/2020, disponible en https://www.senado.gob.ar/parlamentario/comisiones/verExp/3010.17/S/PL

[53] Proyecto de actualización del Código Procesal Penal de la Nación en materia de Informática Jurídica y Criminalística Digital, en línea, consultado el 10/08/2020, disponible en Proyecto de actualización del Código Procesal Penal de la Nación en materia de Informática Jurídica y Criminalística Digital

posibilidad, entre otras cuestiones referentes a la temática, que se introduzca el art. 144 bis redactado de la siguiente manera:

"*Obtención de datos en línea: Ante denuncia fundada de la posibilidad de un delito organizado llevado a cabo por organizaciones criminales y dicha actividad se desarrolle dentro de una red informática cerrada, no accesible por métodos convencionales por parte de terceros o empresas de comunicación, el juez podrá autorizar la realización de operaciones encubiertas por parte de las fuerzas de seguridad bajo las condiciones establecidas en el Artículo 296. La medida tendrá un carácter excepcional y se realizara únicamente a los fines de obtener los medios de prueba necesarios para cesar la operatoria ilícita. Podrá efectuarse por un plazo máximo de treinta (30) días, pudiendo ser renovada, expresando los motivos que justifican la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado. La misma deberá realizarse respetando el derecho a la privacidad e intimidad de terceros no involucrados en el acto criminal dentro de la red informática. La operatoria debe ser supervisada por el Ministerio Público Fiscal. Rige para los funcionarios encargados de efectuar la intervención el deber de confidencialidad y secreto respecto de la información obtenida por estos medios, excepto respecto de la autoridad que la haya requerido. Quienes incumplan este deber incurrirán en responsabilidad penal. La solicitud deberá indicar el plazo de duración que estime necesario según las circunstancias del caso. El juez controlará la legalidad y razonabilidad del requerimiento y resolverá fundadamente. Si los elementos de convicción tenidos en consideración para ordenar la operación desaparecieren, hubiere transcurrido su plazo de duración o ésta hubiere alcanzado su objeto, deberá ser interrumpida inmediatamente.*"[54]

Por su parte, la provincia de Mendoza también cuenta con un proyecto de ley de adecuación de su código procesal penal a la manda del Convenio de Budapest, presentado a fines del año 2018, que pretende incorporar medidas novedosas como el registro remoto de dispositivos electrónicos, tal como lo expresa el art. 216 ter:

"*Registro remoto de dispositivos tecnológicos que contengan evidencia digital: En supuestos urgentes, tratándose de delitos graves, previstos en los artículos 83, 140,*

---

[54] Op. cit.

*141, 142, 142 bis, 145, 145 bis, 145 ter, 146, 147 y 170 en el Título III del Código Penal 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 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) Dia 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*."[55]

He de hacer mención asimismo, al Código Procesal de la Provincia de Neuquén, que prevé el registro remoto electrónico en su art. 153:

"*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*

[55] Proyecto de ley de modificación del Código Procesal Penal de Mendoza, en línea, consultado el 10/08/2020, disponible en https://drive.google.com/file/d/1Pj-Xhjio0MtMfI-1wtrawBIMCD41OpQH/view

*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."*[56]

[56] Código Procesal Penal de la provincia de Neuquén, en línea, consultado el 10/08/2020, disponible en http://www.infoleg.gob.ar/?page_id=87

# VII- Conclusión final

Como ha quedado demostrado a lo largo del presente trabajo, la incidencia de las tecnologías de la comunicación y la información en la vida diaria repercute directamente en el universo jurídico penal. Por un lado, porque han surgido en este tiempo nuevas figuras delictivas ligadas a lo informático, como de igual modo florecen minuto a minuto herramientas disruptivas de las que el Estado -encarnado por los operadores de la justicia y sus auxiliares- puede hacerse para investigar tanto los ilícitos cibernéticos como los tradicionales donde se vea involucrada evidencia digital.

En ese norte, es necesario que las discusiones troncales en torno a la implementación de dichos instrumentos tecnológicos, se encuentren iniciadas mucho antes de su implementación, máxime teniendo en cuenta que estos métodos que implican coerción estatal, se articulan con temas tan sensibles como el derecho fundamental a la intimidad y a la privacidad de las personas. Nótese que aún a riesgo de pecar de pesimista digo “iniciadas” y no “saldadas” puesto que no es mi pretensión arribar a conclusiones definitivas sobre temas cuyo potencial es infinito.

Es esperable que en el futuro aún existan cuestiones que puedan ser materia de debate, y las técnicas hoy propuestas devengan en obsoletas, ya que resulta inverosímil abarcar legislativamente el sinfín de posibilidades que la tecnología es capaz de brindarnos y hoy desconocemos. Sin perjuicio de ello creo que la recompensa de esta regulación se traducirá inmediatamente en una investigación penal más rápida, eficaz y menos susceptible de ser cuestionada.

Considero que no debemos ser temerosos ni reticentes a la hora de estrechar los lazos entre la investigación criminal y las tecnologías disponibles, puesto que aquellos que delinquen no han de hesitar cuando pueden echar mano a nuevas maneras de cometer ilícitos.

Por el mismo andarivel, la circunstancia de que medidas novedosas como la propuesta se encuentren rescatadas por el marco normativo vigente, provoca que sean conocidas por la generalidad de los actores que cumplen un rol en el campo de la investigación y no sean privativas de algunos pocos, más allá de que para su correcta utilización se requiera de una experticia en la materia.

Insisto, y ha quedado demostrado, es **urgente** avanzar en la legislación procesal penal en el ámbito de la provincia de Buenos Aires hacia una reforma integral que prevea la evidencia digital y los medios de prueba digitales en general, y el **registro remoto de dispositivos electrónicos** en particular, de acuerdo a las pautas objetivas expuestas en el capítulo precedente. Su cristalización, como hemos visto a lo largo de la presente labor, implica abundantes beneficios para la administración de justicia así como para los justiciables que podrán conocer de antemano las limitaciones que el Estado debe respetar a la hora de encarar una investigación penal en un entorno digital. Es decir, reglas claras para ambas partes.

En ese sentido, advierto que no resulta suficiente ni provechoso aplicar el principio de libertad probatoria para el manejo de estas herramientas, ni hacer uso análogo de las ya regladas aunque ambos sean recursos utilizados en la práctica. Esto sólo ocasiona serias discusiones en relación a su legitimidad y se pierde de vista que al versar sobre un tipo de evidencia específica, distinta de la tradicional, con características que le son propias, merece un tratamiento específico. Del mismo modo y como ha quedado demostrado, afecta un nuevo estrato de la privacidad, que conjuga todos los demás ámbitos privados conocidos anteriormente.

Por último aunque no menos importante debemos tener en cuenta que con la introducción de esta reforma, habremos satisfecho la deuda internacional que asumimos como Estado al momento de suscribir el Convenio de Budapest, el que como he señalado, recomienda que las legislaciones nacionales de los miembros adopten medidas procesales a los fines de facilitar la investigación penal de los ciberdelitos, de los demás delitos cometidos por medios informáticos y de la obtención de pruebas en formato digital relativas a un delito penal.

# VIII-Bibliografía


- BACHMAIER WINTER, Lorena, Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015, en línea, consultado el 10/02/2020, disponible en https://www.mjusticia.gob.es/cs/Satellite/Portal/1292428206148?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1701_Estudio.pdf&blobheadervalue2=1288794492107.

- BADENI Gregorio, "Tratado de derecho constitucional", 2da ed., La Ley, 2006.
- BERALDI, Carlos A., en Proceso y Procedimientos Penales de la Provincia de Buenos Aires, coordinadores Pedro J. Bertolino y Alberto. Silvestrini, Buenos Aires, Abeledo Perrot, 2013.
- BRUZZONE, Gustavo A., La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal, en Estudios sobre justicia penal, Editores del Puerto, Buenos Aires, 2005.
- CHARTS OF SIGNATURES AND RATIFICATIONS OF TREATY 185 CONVENTION ON CYBERCRIME, en línea consultado el 31/08/2020, disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=5mmNWA6v
- ESCANDAR Nicolás, y FRENCH Santiago en "Injerencias y Estándares Probatorios", Diario DPI Penal N° 93 – 11.12.2015, en línea, consultado el 26/03/2020, disponible en http://www.pensamientopenal.com.ar/system/files/2015/12/doctrina42621.pdf.

- DI IORIO, Ana Haydeé y otros, Buenas prácticas en la extracción y tratamiento de la evidencia digital, Hammurabi, Volumen 2, Buenos Aires.

- GUÍA INTEGRAL DE EMPLEO DE LA INFORMÁTICA FORENSE EN EL PROCESO PENAL, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, en línea, consultado el 02/02/2020, disponible en http://www.pensamientopenal.com.ar/system/files/2019/02/doctrina47360.pdf.

- INFORME EXPLICATIVO DE LA CONVENCION DE BUDAPEST, en línea, consultado el 31/08/2020, disponible en https://rm.coe.int/16802fa403#:~:text=I.,Conferencia%20Internacional%20sobre%20la%20ciberdelincuencia.

- JORGE SANMARTIN, Sara, en El uso de virus espía como diligencia de investigación: análisis crítico y propuesta, año 2016, en línea, consultado el 12/02/2020 en https://gredos.usal.es/bitstream/handle/10366/132691/TFM_JorgeSanMartin_Uso.pdf;jsessionid=D46D7727385CF1585F29F9CE906B386F?sequence=1

- KERR, Orin S. , Serch Warrants in an Era of Digital Evidence, The George Washington University Law School, Public Law and Legal Theory Working Paper Nro. 128, 2005.

- KIEFER, Mariana y VACAREZZA, Tomás, en Evidencia digital: algunos problemas procesales, Temas de Derecho Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, Tribunales, Volumen 3, Buenos Aires, 2015.

- MAIER, Julio B. J. , en Derecho Procesal Penal, Tomo I, Fundamentos, Buenos Aires, Ad Hoc, 2016.

- PIETRO PASTORINO Josefina, "Allanamiento y requisa", en "Medios de prueba en el proceso penal", Volumen 3, Hamurabi, 2018.

- PRESMAN, Gustavo en La Investigación forense informática en América Latina, compilado por Eduardo Ferreyra para la Asociación por los Derechos Civiles, año 2018, en línea, consultado el 10/02/2020 disponible en https://adc.org.ar/wp-content/uploads/2019/06/037-la-investigacion-forense-informatica-en-america-latina-vol-2-04-2018.pdf.

- ROCHA DEGREEF Hugo, "El empleo de la interceptación telefónica como medio de prueba", Revista "El derecho", tomo 143, año 1991.

- SERGI, Natalia, Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina, en Informe realizado para la Asociación por los

Derechos Civiles, en línea, consultado el 02/02/2020, disponible en https://adc.org.ar/wp-content/uploads/2019/06/038-analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina-vol-3-04-2018.pdf

- SUEIRO, Carlos Christian, en La prueba digital en la criminalidad informática: a propósito del nuevo Código Procesal Penal, en Ledesma, Angela, E.; dir, El debido poceso penal: doctrina. Análisis jurisprudencial. Fallos fundamentales, Hammurabi, Volumen I, Buenos Aires, 2016.

# IX- Legislación.


- Ley 11.179, Código Penal de la Nación, publicada en el B.O. de la Nación del 03/11/1921, en línea, disponible en www.infoleg.gob.ar
- Ley 11.922, Código Procesal Penal de la Provincia de Buenos Aires, publicada en el B.O. de la Provincia de Buenos Aires del 23/01/1997, en línea, disponible en www.gob.gba.gov.ar
- Ley 25.326, Protección de datos personales, publicada en el B.O. de la Nación del 30/10/2000, en línea, disponible en www.infoleg.gob.ar
- Ley 26.388 modificatoria del Código Penal de la Nación, publicada en el B.O. de la Nación del 25/06/2088, en línea, disponible en www.infoleg.gob.ar
- Ley 27.319, Delitos Complejos, publicada en el B.O. de la Nación del 22/11/2016, en línea, disponible en www.infoleg.gob.ar
- Ley de Enjuiciamiento de España, en línea, disponible en
- Convenio de Budapest, en línea, disponible en https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Código Procesal Penal de Colombia, en línea, disponible en https://leyes.co/codigo_de_procedimiento_penal.htm
- Código Procesal Penal de Chile, en línea, disponible en https://www.bcn.cl/leychile/navegar?idNorma=176595
- Código Procesal Penal de la provincia de Neuquén, en línea, disponible en http://www.infoleg.gob.ar/?page_id=87
- Proyecto 3010/17 en línea, disponible en https://www.senado.gob.ar/parlamentario/comisiones/verExp/3010.17/S/PL
- Proyecto de actualización del Código Procesal Penal de la Nación en materia de Informática Jurídica y Criminalística Digital, en línea, disponible en http://www.pensamientopenal.com.ar/system/files/2016/08/legislacion43977.pdf
- Proyecto de ley de modificación del Código Procesal Penal de Mendoza, en línea, disponible en https://drive.google.com/file/d/1Pj-Xhjio0MtMfI-1wtrawBIMCD41OpQH/view

# Índice

**Resumen**……..……...……...pg. 4
**Objetivos**…….…….....…….....pg. 4
**Áreas temáticas a trabajar**……..……...……...pg. 5
**Técnicas metodológicas**……...……..pg. 5
**Hipótesis**……...…….....….pg. 5

## CAPITULO I

## LINEAMIENTOS GENERALES

**I.I.** Introducción del tema y su justificación…….…...……...…….....pg. 6

## CAPITULO II

## BREVE RECORRIDO HISTORIO POR NUESTRO SISTEMA DE ENJUICIAMIENTO

**II.I-** Justificación de la mención...…….……..…….....pg. 8
**II.II-** La Inquisición…….……..…….....pg. 8
**II.III-** El Derecho Procesal Penal hispanoamericano.…….....…….....pg. 9
**II.IV-** El Iluminismo y la reforma del sistema inquisitivo.....pg. 9
**II.V-** La situación en la actualidad.....pg. 10

## CAPITULO III

## LAS GARANTIAS PROCESALES RECONOCIDAS CONSTITUCIONALMENTE

**III.I-** Generalidades……..……..…….pg. 12
**III.II-** Límites a la libertad probatoria……..…….pg. 12
**III.II.I.** Referentes a la persona del imputado……..…….……...pg. 13
**III.II.II.** Referentes a la privacidad y al derecho a la intimidad de la persona……..pg. 14

## CAPITULO IV

## EL SISTEMA PROBATORIO EN EL CODIGO PROCESAL PENAL DE LA PROVINCIA DE BUENOS AIRES

**IV.I-** Consideraciones generales……..…….pg. 17
**IV.II.-** La libertad probatoria ……..……..……pg. 18
**IV. III.** La valoración de la prueba……..……..……...…pg. 19
**IV.IV.** Las exclusiones probatorias..……..……..……..…….pg. 19
**IV.V.** Los medios de prueba regulados expresamente……...……..pg. 19
**IV.V.I**. El registro domiciliario…….……..……..pg. 20
**IV.V.II.** La interceptación de correspondencia……...……..pg. 23
**IV.V.III.** La intervención de comunicaciones telefónicas…...…….pg. 24

## CAPITULO V

## LA EVIDENCIA DIGITAL

**V.I-** Definición……..……pg. 26
**V.II.** La regulación normativa de la evidencia digital……...……pg. 29
**V.III.** La convención sobre la ciberdelincuencia de Budapest……...…..…pg. 30
**V.III.I.** Antecedentes del Convenio sobre ciberdelincuencia de Budapest...pg. 30
**V.III.II.** Finalidades y conformación del Convenio……..…….pg. 32
**V.III.III.** Terminología del Convenio……..…..……pg. 33
**V.III.IV.** Medidas procesales recomendadas por la Convención…….……pg. 36
**V.IV.** El contexto normativo en Latinoamérica……...….pg. 40
**V.V.** Protocolo para la preservación, obtención y análisis de la evidencia digital de la provincia de Buenos Aires……...…..….pg. 41

## CAPITULO VI

## EL REGISTRO REMOTO DE DISPOSITIVOS ELECTRONICOS

**VI.** El registro remoto de dispositivos electrónicos…….…….pg. 46
**VI.I.** Métodos mediante los cuales puede llevarse a cabo la medida……...……pg. 51
**VI.II.** Pautas objetivas a tener en cuenta para su aplicación……...……....pg. 54
**VI.III.** El registro remoto de dispositivos en el derecho comparado……pg. 55

**VII.** Conclusión final……..……..……..……..…....pg. 61

**VIII.** Bibliografía……...……..……..……pg. 63

**IX.** Legislación.……....…….....pg. 66

**Carta al tutor**

Dr. Hernán Moyano:

Me dirijo a Usted, como alumno de la carrera de Abogacía de la Facultad de Derecho y Ciencias Políticas de la U.A.I, localización Centro, turno noche, a los efectos de solicitarle quiera tener a bien aceptar su designación como tutor de tesis, la cual será presentada para someterse a corrección ante la Secretaria Técnica de dicha facultad, sita en la calle Chacabuco N° 90, piso 6° de la Ciudad Autónoma de Buenos Aires, el día de octubre de 2019.

En tal sentido le informo que el tema a desarrollar será "....." y que el mismo fue aceptado por la Secretaria Administrativa anteriormente mencionada.

Asimismo, en caso de que acepte la referida designación, solicito su asistencia y supervisión técnica para llevar a cabo este trabajo final, de manera correcta.

Sin otro particular, saludo a Ud. muy atte.

Agustín Miguel Eusebio