Maestría en Derecho Penal

Departamento de Derecho

Evidencia informática: ¿Un nuevo paradigma para el derecho procesal penal?

Natalia Schirakian

DNI: 36.592.614

Tutor de tesis: Abogado, Marcos Salt

Buenos Aires 30 de junio de 2021

***Abstract*/resumen**

Se puede observar que en los Códigos Procesales Penales de nuestro país, en general, no se encuentran previstos los medios de prueba específicos para poder incorporar la evidencia digital a las investigaciones penales. Ante la falta de regulación, los operadores del sistema judicial se han visto obligados a incorporar este tipo de evidencia a través del principio de "libertad probatoria", utilizando la analogía como herramienta principal. Este escenario trajo consigo significativos problemas, toda vez que se vieron vulnerados derechos y garantías de los ciudadanos. Es por ello que la pregunta que debemos efectuarnos es si, ante la falta de regulación, es posible un proceso penal respetuoso de las garantías y derechos del imputado.

Palabras calves

Nuevas tecnologías – tecnologías de la información (TIC) – libertad Probatoria - analogía- *nulla coactio sine lege*- – derechos del imputado - evidencia digital- dato electrónico – medidas probatorias

INDICE TEMÁTICO

Introducción

En el presente trabajo ilustraré cómo el avance de las tecnologías informáticas, más precisamente las tecnologías de la comunicación (TIC), han traído aparejados un sinfín de cambios en el ordenamiento procesal penal. En concreto, buscaré demostrar la necesidad imperante de un cambio radical dentro del ordenamiento procesal penal, más específicamente, la necesidad de regular la incorporación de la evidencia digital al proceso penal.

El avance de estas nuevas tecnologías afectó en un todo al ser humano. Hoy en día existen dispositivos electrónicos que almacenan muchísima información de la vida privada de las personas lo que, en virtud de la falta de regulación procesal penal específica, puede traer aparejado innumerables conflictos a la hora de recabar información en el marco de una investigación penal.

En nuestro país, tal como se verá en el presente trabajo, los medios de prueba se encuentran diseñados para recolectar evidencia física y no evidencia digital, esta última incorpora al proceso penal a través del principio de libertad probatoria, sobre la aplicación de la analogía.

Si bien en los últimos años, en virtud del avance tecnológico, se han desarrollado nuevas conductas que exigirían la necesidad de una tipificación penal, no es ocioso recordar que, en lo que hace a la materia penal sustantiva, si existieron numerosas actualizaciones. Un claro ejemplo de ello fue la Ley N° 26.388 del 4 de junio del año 2008. Esta ley modificó nuestro Código Penal, para así incluir distintas conductas como típicas, entre ellas el ofrecimiento y distribución de pornografía infantil (CP, art. 128); conductas relativas a la violación de secretos y la privacidad que incluyen el acceso ilegítimo a sistemas informáticos ajenos; la intercepción de correspondencia electrónica y otras formas de comunicación; la revelación de secretos y los delitos relacionados con la protección de datos personales (CP, arts. 153, 153 bis, 155, 157 y 157 bis); entre otros.

En concreto, en el derecho penal material, a diferencia de lo ocurrido en el derecho procesal penal, se advirtió más rápido la necesidad de un cambio radical motivo por el cual, se efectuaron modificaciones en los Códigos Penales a fin de tipificar, de

manera específica y en respeto al principio de legalidad penal, estas nuevas conductas disvaliosas que, hasta ese momento, resultaban atípicas.

Es en virtud de todo lo expuesto que, en el marco del presente trabajo, buscaré exponer de manera específica el conflicto que trae aparejado la falta de regulación de los medios de prueba para incorporar la evidencia digital y la necesidad imperante de una modificación sustancial de los códigos procesales penales, es decir, un cambio de paradigma procesal. Para ello, señalaré la problemática que conlleva el mentado principio de libertad probatoria aplicado a medidas probatorias no reguladas que, en la práctica, se traducen en una aguda injerencia en derechos fundamentales de las personas.

I – Tecnologías informáticas y las modernas tecnologías de la comunicación (TIC). ¿Qué desafíos conllevan?

A- Nuevas tecnologías informáticas

En la actualidad, se discute arduamente el alcance de los medios de prueba tradicionales en materia penal a la luz de los avances tecnológicos. Es decir, el avance de estas nuevas tecnologías trajo aparejado numerosos cambios los que, a su vez, se tradujeron en una necesidad de poder armonizar los textos normativos a esta nueva realidad.

Es conocido que, desde las últimas décadas del siglo XX, los avances científicos y tecnológicos han sido los protagonistas en la vida de los seres humanos. Los usos de las nuevas tecnologías de la información y de la comunicación han incrementado notoriamente la gestión de la información, ya sea desde los modos de comunicación tradicionales hasta el abundante caudal de información que hoy en día circula por las redes. En ese sentido, la información se ha convertido en poder y se ha posicionado en la base del progreso social y de la humanidad, pasando de las meras llamadas telefónicas o de fax hasta la revolución tecnológica que significó internet donde la información es transmitida y recibida a través de una red universal a todos los ciudadanos.

Las tecnologías de la información y la comunicación pueden definirse como "el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarca las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro"[1].

Esta revolución tecnológica ha significado una modificación radical para toda la sociedad y, en consecuencia, para los sistemas penales y procesales penales. Su llegada y ulterior desarrollo exigió cambios significativos en el sistema poniendo en jaque las normas procesales y penales, los principios jurídicos e incluso la manera en la cual se llevaba a cabo la investigación.

Esta situación, sumada a que los Códigos Procesales Penales únicamente tienen medios probatorios pensados para la incorporación de evidencia física, se tradujo en un gran problema para la investigación y represión de delitos puesto que, más allá de

[1] SALT, *Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ad Hoc, 2017, p. 11.

la falta de regulación, han aparecido nuevos medios de prueba necesarios para la investigación y posterior represión de los delitos en la sociedad que vivimos hoy en día. Es decir, la llegada de este nuevo mundo tecnológico habría exigido un cambio radical del sistema procesal penal lo que, como veremos a continuación, no sucedió.

Por otro lado, y en lo que hace al derecho penal de fondo, podríamos decir que no sucedió lo mismo puesto que, en virtud al principio de legalidad penal, los sistemas penales han adaptado sus códigos en virtud de estos "nuevos delitos". Un claro ejemplo es la ley n° 26.388, sancionada en el año 2008, de nuestro país, la cual reguló una serie de delitos penales informáticos. En ese sentido, Salt (2017) resalta que la importancia del principio de legalidad penal en los países de tradición europea continental fue el principal protagonista en este disparejo desarrollo entre lo que hace a la actualización del Derecho Penal y el Derecho Procesal Penal a la hora de hacer frente a los nuevos desafíos de la sociedad moderna

En cuanto a la regulación procesal penal, los cambios fueron más lentos "primando la pretensión de aplicar las normas tradicionales que regulan la prueba en el proceso penal pergeñados pensando en la prueba "física" a los nuevos elementos y medios de prueba sustentados en tecnología informática (…) basándose fundamentalmente en el principio de libertad probatoria reconocido en la mayoría de las legislaciones (…) sobre la base de la aplicación analógica de las reglas que regulan los medios de prueba tradicionales"[2].

El avance de estas tecnologías se traduce hoy en una amenaza a las garantías individuales si no se cuenta con un Estado presente que se encargue de regular estos nuevos escenarios conforme a derecho. En conclusión y, más allá de la regulación o falta de regulación de los nuevos escenarios que han traído esta revolución informática, lo que no se puede negar es que esta nueva realidad llegó para quedarse y es por ello, que la normativa procesal penal deberá adaptarse a ella.

B- Principio de Libertad probatoria y medios de prueba.

Una primera pregunta que debemos hacernos es si la regulación procesal penal vigente les brinda a los operadores judiciales el marco de legalidad necesario para efectuar investigaciones en entornos digitales, empleando medios de prueba no reglados para

[2]Véase, SALT, "*Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos"*, 2017, p. 16.

incorporar al proceso penal la evidencia digital. Se puede observar que nuestros códigos procesales no cuentan con una regulación pertinente en medidas probatorias para la incorporación de evidencia digital, es por ello que deberíamos indagar si nuestros sistemas procesales nos brindan un sistema abierto o un sistema cerrado en lo que hace a la materia probatoria.

Nuestros sistemas procesales penales, casi en su mayoría, proponen un sistema abierto en cuestiones probatorias. A modo de ejemplo, el Código Procesal de la Ciudad Autónoma de Buenos Aires en su Artículo 112 reza: "Los hechos y las circunstancias de interés para la solución correcta del caso **podrán acreditarse por cualquier medio de prueba que no resulte contrario a los principios contemplados en este Código**"-el destacado me pertenece-. A su vez, el Artículo 192 del Código Procesal Penal Cordobés (CPPC) establece que "Todos los hechos y circunstancias relacionados con el objeto del proceso pueden ser acreditados por cualquier medio de prueba, salvo las excepciones previstas por las leyes" y el Artículo 193 del CPP de la Nación "La instrucción tendrá por objeto: 1°) Comprobar si existe un hecho delictuoso mediante las diligencias conducentes al descubrimiento de la verdad", entre otros.

La falencia de regulación en el ámbito del derecho procesal penal en relación a la evidencia digital ha sido suplida a través del principio de libertad probatoria. Este principio se remonta a épocas pasadas en las que se buscaba superar el sistema de prueba tasada y, por ese motivo, se procuraba poder acceder a la verdad a través de cualquier medio que no vulnerara principios y garantías constitucionales.

En cuanto a la libertad probatoria, se podría esbozar que es un principio del cual se desprende que "en materia procesal penal, todo puede probarse y por cualquier medio, y que por lo tanto es posible, para probar un hecho, acudir a un medio de prueba no reglado específicamente en la ley procesa, debiéndose en todo caso aplicar analógicamente las normas procesales que más similitud tengan con el medio de prueba extraño a la codificación. La idea central, entonces, es que la regulación de los medios de prueba en los códigos procesales no es taxativa"[3].

1- Primer obstáculo, analogía en perjuicio del imputado

[3]Pérez Barbará, "Nuevas tecnologías y libertad probatoria en el proceso penal" en *Nueva Doctrina Penal (NDP)*, N°1, 2009, p. 273

Cabe aclarar que la aplicación analógica en lo que hace al derecho penal de fondo no se puede efectuar en perjuicio de la persona sometida al proceso penal por el principio de legalidad penal contenido en el artículo 18 de nuestra Constitución Nacional. Este principio, del cual se desprende la imposibilidad de efectuar una interpretación analógica de las normas en perjuicio del imputado, se aplica de manera ilimitada al derecho penal de fondo, pero ¿sucede lo mismo en materia procesal penal? o, por el contrario, se aplica de manera limitada.

Una postura podría ser que "en el ámbito penal, la aplicación analógica tanto de la ley penal material como de la ley procesal penal está admitida sin discusión siempre que sea *in bonam partem* (…) en materia procesal penal, sin embargo, la legislación prohíbe expresamente la aplicación analógica sólo en los casos en que esté en juego la libertad ambulatoria del imputado o cuando se trate de una norma que restrinja alguna de sus facultades o poderes"[4].

Conforme a lo expuesto, podría entenderse que, desde una postura más restrictiva, la prohibición de la aplicación analógica en perjuicio del imputado es absoluta en lo que refiere a derecho penal sustantivo y relativo en lo que hace al derecho penal procesal. Esa postura estaría basada en "la propia letra de la Constitución, que establece que nadie puede ser ´penado" sin ley previa. Pero la razón material que explica incluso el texto constitucional está dada por el carácter de la sanción propia del derecho penal: la pena, en tanto constituye la forma más violenta de reacción estatal, y se exige, por lo tanto, como presupuesto de ella, requisitos más estrictos que los que pueden ser suficientes para legitimar la aplicación de normas jurídicas no penales. La prohibición de la analogía *in malam parten* (…) como consecuencia del principio de legalidad penal, tiene por objeto proteger al ciudadano en contra de la posible arbitrariedad estatal"[5].

Pero ahora deberíamos preguntarnos, ¿existe arbitrariedad en el proceso penal si la pena que finalmente se impone se basa en un proceso en el cual fueron empleados medios de coerción no regulados? La respuesta es sí.

Es por ello que podríamos afirmar, en lo que hace a materia procesal penal, que también debe regir de manera amplia el principio de prohibición de analogía en perjuicio del imputado. No podría emplearse la analogía en una medida de prueba que signifique una coerción en el proceso penal que no esté regulada y que, a su vez, perjudique la situación

[4]Pérez Barberá, "Nuevas tecnologías y libertad probatoria en el proceso penal" en *N.D.P*, 2009, p. 274.
[5]Pérez Barberá, "Nuevas tecnologías y libertad probatoria en el proceso penal" en *N.D.P*, 2009, p. 275.

procesal del imputado en el caso en concreto. El principio de libertad probatoria nos permite observar que la regulación que existe en los códigos procesales claramente no es taxativa, pero tiene límites. Eso se traduce en que no es absoluto y, en ese sentido, no podría avalar la incorporación al proceso penal de elementos probatorios que signifiquen una violación a garantías constitucionales o que estén expresamente prohibidos por ley.

La prueba será admitida cuando ingresa al proceso por algún medio que se encuentre regulado o a través del principio de libertad probatoria, siempre y cuando no se vean afectadas garantías constitucionales. El Estado no puede emplear cualquier medio de prueba que se encuentre a su alcance a fin de llevar a cabo una investigación penal, sino que, únicamente, podrá emplear aquellos medios que sean incorporados al proceso conforme a derecho.

En este mismo sentido, Bruzzone (2005) afirma que, más allá del *numerus apertus* en lo que hace a la materia probatoria y a los casos expresamente descartados por el legislador, también existen límites que emanan de los principios generales. Es decir, si la medida probatoria pone en jaque derechos o garantías constitucionales, estamos frente a una medida coercitiva y, como tal, no puede ser empleada sin limitaciones. Más allá de que existe un *numerus apertus* en lo que hace a medidas probatoria no sucede lo mismo en las medidas de coerción[6].

2- ¿Se puede emplear la analogía para dos objetos de prueba antagónicos?

Para empezar, debemos resaltar que, si pensamos en aplicar analógicamente medidas probatorias empleadas para elementos físicos a evidencia digital, estaríamos empleado sistemas pensados para pruebas que difieren ontológicamente. En ese sentido, claro está que no es lo mismo registrar una casa en búsqueda de una cosa física que registrar un teléfono en búsqueda de un dato ya que estaríamos aplicando analógicamente medidas probatorias para dos escenarios completamente distintos.

Una gran diferencia puede establecerse en que el objeto de la evidencia digital, a diferencia de la evidencia física, es el dato electrónico. Este no es visible a las personas, requiere conocimiento específicos de especialistas de la materia, es frágil y volátil, es decir que todo el tiempo puede ser alterado modificado e hasta incluso eliminado. En ese mismo sentido, los datos electrónicos son masivos, lo que quiere decir que podemos encontrar una

[6] Véase BRUZZONE, Homenaje al profesor Julio B. J. Maier estudios sobre justicia penal *La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso pena"*, Buenos Aires, Editores del Puerto, 2005, p. 8.

infinidad de datos en cada dispositivo. Por último, es dable resaltar que estos pueden ser copiados sin límites, en conclusión, los datos pueden ser clonados.

En conclusión, podemos advertir que uno de los motivos por los cuales no se puede emplear la analogía entre la evidencia física y la digital tiene que ver básicamente con que no son situaciones análogas. En concreto, no existen medidas de pruebas análogas porque el objeto de prueba sobre el cual se deberían aplicar es de distinta naturaleza.

3- Medios de prueba y medidas coercitivas. Principal límite al principio de libertad probatoria: "*nulla coactio sine lege*"

En palabras de Maier, se podría definir a los medios de prueba como el procedimiento regulado por ley, a través del cual se introduce en el proceso penal un elemento de prueba y a su contenido. A su vez, el elemento de prueba, será aquel dato, rastro o señal, contenido en un medio de prueba ya realizado que conduce de manera directa o indirecta a un conocimiento cierto o probable del objeto del procedimiento.[7]Ahora bien, cuando estos medios de prueba conllevan una injerencia en derechos y garantías de los ciudadanos son considerados medios de coerción.

En ese sentido, podríamos esbozar que el principio de la libertad probatoria rige únicamente para los medios de prueba, toda vez que, si la medida se traduce en una injerencia en derechos y garantías del imputado, estaríamos hablando de medidas coercitivas y, en ese sentido, no se podrá emplear este principio.

Aclarado ello, es importante mencionar que otro límite que tiene la libertad probatoria es el principio de *nulla coactio sine lege.* Este deriva del principio constitucional del *nullum crimen* y se traduce en que no puede aplicarse una coacción si la misma no se encuentra expresamente prevista en la ley procesal, con sus alcances y supuestos de aplicación. El principio de *nulla coactio sine lege* se encuentra expresamente previsto en el artículo 30 de la Convención Americana de Derechos Humanos, el cual reza: *"*Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas". Es decir, si tomamos cualquier medida de coerción que no se encuentre prevista en la ley

[7] MAIER, *Derecho Procesal Penal* Tomo I, 2.a ed., 3.a reimpresión, Buenos Aires, Editores del Puerto s.r.l., 2004, p. 859.

procesal o que simplemente no esté para ese mundo de casos, estaríamos violando el mandato del art. 30.

Una medida probatoria informática que no se encuentra contemplada en los códigos de procedimiento y, a su vez, implique de una u otra manera una injerencia por parte del estado en el ámbito de las garantías reconocidas por la Constitución Nacional o los Pactos internacionales de Derechos Humanos con esa jerarquía, no debería ser admitida en el marco del proceso penal.

A su vez, como ya es sabido, estas leyes procesales deberán elaborarse conforme a los requisitos propios de la reglamentación constitucional, la que exige que el legislador no altere, sustituya o modifique el principio constitucional que está reglamentando (CN, arts. 14, 19 –segunda parte- y 28 y, de manera expresa, en el art 30 de la Convención Americana de Derechos Humanos). Conforme a este principio las actividades probatorias del Estado en el marco de los procesos penales que se traduzcan en una injerencia en garantías y derechos fundamentales de los ciudadanos tienen, como condición de legitimidad, una autorización legal previa[8].

A modo de aclaración, debo destacar que la Corte Interamericana de Derechos humanos, define el término ley a la luz del art. 30 de la Convención de la siguiente manera: "que la palabra leyes en el artículo 30 de la Convención significa norma jurídica de carácter general, ceñida al bien común, emanada de los órgano legislativos constitucionalmente previstos y democráticamente elegidos, y elaborada según el procedimiento establecido por las constituciones de los Estados Partes para la formación de las leyes"[9].

En este punto, es interesante destacar las conclusiones a las que arriba Bruzzone (2005) en relación a los requisitos que son necesarios para que una medida coercitiva sea válida. Éstos) son: "1) tiene que estar prevista en la ley (*nulla coactio sine lege*); 2) Que el órgano que la está dictando en ese momento determinado, es el competente para disponerla; 3) Que la medida sea necesaria; 4) Que la medida es idónea para el fin que persigue; y 5) por último, que la medida sea proporcional teniendo en cuenta los intereses afectados"[10].

[8]Véase, SALT, *Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, 2017, p.45.
[9]Texto completo disponible en https://corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf
[10] Véase BRUZZONE, Homenaje al profesor Julio B. J. Maier estudios sobre justicia penal en *La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso pena"*, 2005, p. 12.

Entiende que debemos acudir a estos parámetros cada vez que empleemos una medida de injerencia o de coerción; primero, para fundarlas; luego, para poder criticarlas cuando entendamos que no se deben utilizar; y, finalmente, para controlarlas. El objetivo final es efectuar una unificación de criterios, para así aproximarnos a una "teoría general de las medidas de coerción"[11].

[11]Véase BRUZZONE, Homenaje al profesor Julio B. J. Maier estudios sobre justicia penal en *La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso pena"*, 2005, p. 12.

I- Diferencias esenciales entre la evidencia física y la evidencia digital, su incorporación en el proceso

El avance a pasos agigantados de la revolución tecnológica ha traído no solo cambios en la vida diaria de los hombres y mujeres, sino que también ha venido a modificar al derecho penal y al derecho procesal penal, Constituyendo un nuevo tipo de evidencia en los procesos penales.

Para empezar, entenderemos por prueba a "todo aquello que en el marco de un procedimiento penal y de sus reglas, produce en quien interviene en él un conocimiento cierto o probable acerca de la hipótesis contenido del procedimiento, la imputación a una persona de un hecho punible"[12].

Se entiende que la evidencia digital o evidencia electrónica es aquella información en materia probatoria en la que su relevancia en el proceso penal dependerá del contenido del dato electrónico, de su ubicación en un dispositivo determinado o del hecho de haberse transmitido a través de una modalidad informática o telemática. Asimismo, la Guía de Prueba Electrónica del Consejo de Europa la define como "aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tiene relevancia en un procedimiento judicial". Ahora bien, de manera estricta, la evidencia digital se entiende como un tipo de evidencia electrónica, más allá de que ambos términos se emplean como sinónimos.

En sentido estricto, Salt resalta que "la denominada evidencia digital es en realidad un tipo de evidencia electrónica (concepto más amplio) aunque en muchas ocasiones son utilizados como sinónimos. El término evidencia electrónica incluye forma de datos análogos como fotos, audios o videos que pueden ser digitalizados y asumir formatos digitales, aunque en su origen no lo eran. Por este motivo, algunos autores prefieren poner el acento en el concepto más amplio de la evidencia electrónica (incluyendo los datos análogos y digitales que adquieren la forma de datos digitales) como los datos en formato digital que son creados, manipulados, almacenados o comunicados por cualquier dispositivo informático o

[12] VÉLEZ MARICONDE, *Derecho Procesal Penal*, Tomo III, Parte General, Actos procesales, Buenos Aires, Editores del Puerto, 2011, p. 81.

sistema informático o transmitidos por un sistema de comunicaciones y que tienen relevancia para un proceso"[13].

A su vez, la información recabada, es decir este dato digital, es volátil, inmaterial, modificable y reproducible. Lo mencionado hace referencia a que, a diferencia de la evidencia física, la evidencia digital puede ser fácilmente dañada o destruida, aún de manera involuntaria, toda vez que se requiere de conocimientos específicos para poder manipularla.

Claramente, esta nueva categoría probatoria requiere cuanto menos una adecuación normativa importante tanto en lo que hace al Derecho Procesal Penal y de los mecanismos de cooperación internacional. Es manifiesto que esta nueva evidencia digital es radicalmente distinta a la evidencia física, lo que genera la necesidad imperante de una nueva regulación. Hoy en día este tipo de prueba no se limita únicamente a los "delitos informáticos en sentido estricto", sino que, con los avances tecnológicos, se ha extendido a la investigación de cualquier tipo de delito. Es más, entiendo que, en un futuro no tan lejano, la evidencia física se irá reemplazando por la evidencia digital toda vez que, ésta es mucho más fiable.

En la actualidad, para la incorporación de estas medidas probatorias y ante la falta de regulación, se recurre al principio de libertad probatoria y, por lo tanto, a la aplicación analógica que regula las medidas de pruebas tradicionales, es decir, las medidas de prueba sobre evidencia física. La aplicación analógica en este tipo de procesos, más allá de los cuestionamientos a nivel constitucional que se le podrían efectuar, presenta problemas en la eficiencia estatal de investigación de los delitos y, por otro lado, imposibilita una adecuada protección de las garantías constitucionales de los imputados y de terceros que se pudieran ver afectados por la actuación del estado en el marco de un proceso penal[14]

[13]Véase, SALT, "*Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos"*, 2017, p.31
[14]Véase, SALT, "*Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos"*, 2017, p.17.

III.- Medidas probatorias

A- Retención de datos de tráfico

La retención de datos de tráfico refiere a aquella medida que obliga a los proveedores de los servicios de internet y comunicaciones a conservar los datos de tráfico por determinado período de tiempo aún sin estar vinculados a una investigación penal concreta. Es una medida legislativa de carácter general en la que, como veremos a continuación, la garantía de la intimidad y la privacidad de las personas puede verse afectada.

La medida obligar a las empresas proveedoras de servicio de internet a almacenar datos de tráfico de las comunicaciones efectuadas por los usuarios por un período determinado de tiempo con el objetivo de que puedan ser empleadas por los órganos de persecución penal a fin de poder llevar a cabo el proceso[15].

El gran problema que presenta es, como se ha advertido, la posible injerencia en los derechos de las personas, principalmente, el derecho a la vida privada, la intimidad y a los datos personales. Por este motivo, la misma debe encontrarse estrictamente delimitada y, en ese sentido, debe ser empleada cuando sea sumamente necesario para la investigación de delitos que, por su gravedad, así lo demanden.

En el marco de la Convención de Budapest se buscó, a lo largo de los años de discusión de la misma, prever una medida para retención de datos. Sin embargo los países no se pudieron poner de acuerdo toda vez que era notable que la mentada medida afectara la privacidad de los ciudadanos. No obstante ello, y a raíz de los atentados sucedidos a inicios del presente siglo[16], varios países de la Unión Europea divisaron la necesidad de regular la mentada medida.

En el caso de Argentina, el análisis de la medida se remonta a fines del año 2003 cuando el Congreso sancionó la ley 25.873 por la cual se modificaba la Ley de Telecomunicaciones n° 19.798. En esa oportunidad, se puso el foco en la responsabilidad de los prestadores de servicios de telecomunicaciones respecto de la captación y derivación de las telecomunicaciones para su observancia por parte del Poder Judicial o Ministerio Público.

---

[15]Véase PORTILLO, "*Aseguramiento vs. retención de datos de tráfico de las comunicaciones electrónicas"*, en FERRER (comp) Estudios de Cibercrimen, Buenos Aires, Olejnik, 2021, p 119 y sig.
[16]Atentado a las torres gemelas del 11/9/2001, atentado al tren de España del 11 de marzo de 2004 y atentado al tren de París del 21/8/2015.

La reforma normativa, en su artículo primero, rezaba: "todo prestador de servicios de telecomunicaciones deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público"[17]. Sumado a ello, hacía cargar con los costes de dicha obligación a los prestadores y les exigía que almacenen y clasifiquen los datos relativos a la identificación de los usuarios y a los datos relacionados al tráfico de las comunicaciones por un plazo de diez años[18].

Esta ley no contaba con las disposiciones necesarias a fin de brindar un estándar de seguridad para proteger la intangibilidad de los datos almacenados, ni establecía un lugar geográfico dónde se debía almacenar esos datos a fin de garantizar la jurisdicción. Fue por todas estas falencias que, finalmente, el P.E.N. suspendió su aplicación a través del Decreto n° 357/05. Ahora bien, este contexto llevó a la discusión de la mentada medida y, en concreto, al análisis de su falta de compatibilidad con el sistema jurídico, en ese momento vigente. Concretamente esta discusión se llevó a cabo en el fallo "Ernesto Halabi c/ P.E.N de la Corte Suprema de Justicia (Arg.) de fecha 24 de febrero de 2009.

En aquella ocasión, Halabi presentó un recurso de amparo contra el P.E.N. en el cual reclamaba que se declare la inconstitucionalidad de la ley 25.873 y su decreto reglamentario 1563/2004 por considerar que sus disposiciones vulneran las garantías establecidas en los artículos 18 y 19 de la Constitución Nacional, toda vez que se autorizan las intervenciones a las comunicaciones telefónicas y por internet sin que se encuentre estipulado en qué casos y con qué justificativos.

Finalmente, se hizo lugar al amparo promovido por Halabi y se declaró la inconstitucionalidad de las disposiciones de esa norma basándose en la falta de debate legislativo suficiente previo al dictado de la mentada ley. Lo que se podía observar era la vaguedad de la mentada normativa, toda vez que no se especificaba en qué medida se podía

[17]Texto disponible en *http://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/92549/norma.htm*

[18]En este sentido, es necesario efectuar una distinción entre los distintos tipos de datos informáticos, con sus distintas relevancias en pos de sus características e injerencias en los derechos y garantías de las personas, en concreto tenemos: a. Datos de abonado: Son los datos necesarios para identificar a un usuario determinado, por ejemplo a fin de conocer a quien pertenece determinada IP en un determinado momento, o un número telefónico, datos de facturación, todo lo que puede tener registrado. Es decir es el tipo de dato más "básico" que, generando no tanta injerencia en el ámbito de la vida privada de las personas, nos brinda información muy valiosa para el proceso. b. Datos de tráfico: Son los datos referidos a la comunicación, aquel destinado a identificar una comunicación específica y, c. Datos de contenido: Son los datos referidos al contenido propio de la comunicación

captar el contenido de las comunicaciones sin autorización judicial, es decir, no existían los estándares mínimos de seguridad exigidos para este tipo de medidas.

En instancias del análisis de la validez de la nombrada ley, por la cual las empresas de telecomunicaciones estarían obligadas a almacenar los datos de sus usuarios durante un plazo de diez años para tenerlos a disposición del Ministerio Público Fiscal y del poder Judicial, la Corte Suprema de Justicia, señaló que "las comunicaciones electrónicas y todo lo que los individuos transmiten por estas vías, forman parte integrante del derecho a la intimidad personal. A partir de esa tesitura, señaló que la garantía consecuente de dichos derechos actúa contra toda injerencia o intromisión arbitraria o abusiva en la vida privada de los afectados. Desde este punto de vista, no alcanza con la virtuosa finalidad que tenga una norma para ser considerada válida, sino que, además y principalmente, los medios elegidos para dicha finalidad deben ser acordes y respetuosos a los derechos fundamentales"[19].

Por último, es importante destacar que la doctrina central que este fallo dejó en el ámbito nacional es el haber asimilado los datos de tráfico a los datos de contenido. En conclusión, esto permite observar que tanto los datos de tráfico como los datos de contenido cuentan con la misma protección, motivo por el cual debe efectuarse un mismo tratamiento a la hora de ingresarlos al proceso penal.

Ahora bien, volviendo al ámbito europeo, es necesario resaltar que en el año 2006 la directiva n° 24 del Parlamento y Consejo Europeo obligó a los países a que incorporen una medida de retención de datos de tráfico. En concreto, se planteó que la conveniencia de que todos los países de la región incorporen la regulación de retención de datos de tráfico.

No obstante ello, en los países en los que se reguló y sancionó esta medida, se empezó a observar que la misma resultaba inconstitucional. Es decir, se empezó a agudizar el enfoque hacia la protección de las garantías y, en ese sentido, algunos países empezaron a advertir la dificultad que representaba esta acumulación de datos personales por parte del Estado y decidieron modificar su accionar e implementar la medida de la conservación de datos. Sin embargo, otros países como España, continúan insistiendo con la regulación de la medida.

[19]PORTILLO, "*Aseguramiento vs. retención de datos de tráfico de las comunicaciones electrónicas"*, en FERRER (comp) Estudios de Cibercrimen, 2021, p 119 y sig.

B- Aseguramiento inmediato de datos informáticos almacenados.

Esta medida se encuentra estipulada en el artículo 16 del Convenio sobre la Ciberdelincuencia (de ahora en más, "Convención de Budapest") y, al igual que la conservación y divulgación inmediata de los datos de tráfico, se aplican a datos que ya se encuentran almacenados y conservados por los titulares de los mismos.

Tal como lo señala Salt, la presente es una medida cautelar probatoria que faculta a las autoridades de los estados partes a requerir a un tercero el aseguramiento de los datos que posee en su sistema informático. De ninguna manera eso se traduce en que deba exhibir o exponer el dato, sino que únicamente debe garantizar que éste no va a ser afectado durante determinado tiempo. De esta manera, se impide que los datos sean alterados o borrados.

Como se mencionó anteriormente, la característica de volatilidad que poseen los datos informáticos conlleva la necesidad de emplear esta herramienta en los comienzos de la investigación penal a fin de evitar que sean destruidos o alterados en alguna manera y así, preservar o asegurar los datos existentes en los soportes digitales o técnicos.

No es una medida que se aplique a la obtención en tiempo real de datos ni para la conservación de los datos relativos al tráfico en el futuro, tampoco a lo que hace al acceso en tiempo real a los distintos contenidos de las comunicaciones, sino que únicamente se aplica a los datos informáticos ya existentes y almacenados.

En ese sentido, el informe explicativo de la Convención de Budapest refiere que la mentada medida requiere que los datos que ya existen y se encuentran almacenados de alguna manera, se puedan proteger contra todo aquello que pueda causar que su calidad o condición actual sufra algún tipo de cambio, deterioro o eliminación. Esta no requiere que los datos sean inaccesibles o que queden inutilizados[20].

La persona a quien se dirige la orden tendrá la obligación de conservar y proteger la integridad de los datos de manera confidencial durante el tiempo que las autoridades estimen necesario, con un máximo fijado en los noventa días, con el fin de que las autoridades competentes, en caso de ser necesario, puedan exigir su revelación. A su vez, el reporte explicativo invita a cada estado parte a que especifique el plazo máximo durante el cual los datos deberán ser conservados, y establece que, la orden de la mentada medida, deberá

[20]Explicación brindada por los integrantes del Comité de Ministros del Consejo de Europa en el Informe explicativo del Convenio sobre Ciberdelincuencia aprobado el 8 de noviembre de 2001 -ver Acápite 159-.

especificar claramente cuál será el lapso por el cual los datos deberán quedar conservados, teniendo como límite máximo el término de 90 días. No obstante ello, la parte podrá solicitar la renovación de la mentada orden.

Asimismo, se impone la obligación a la persona que custodia los datos de mantener en silencio los procedimientos de conservación de datos. Esto se debe a la necesidad de que el sospechoso de la investigación no tenga conocimiento del proceso en curso. La importancia del secreto reside en la necesidad de que los datos no sean borrados o alterados.

Entonces, la finalidad de esta medida es asegurar determinada información para que, con posterioridad y en caso de ser necesario, pueda ser incorporada a proceso, motivo por el cual, en principio, no vulnera los derechos a privacidad de los usuarios. Los datos podrán o no ser requeridos con posterioridad por la autoridad, es decir, su conservación es independiente de su incorporación o no a determinado proceso penal. Esta medida solo atañe a la conservación del dato, es decir aquí no se va a pedir agregar el dato al proceso, exponerlo o divulgarlo, sino que únicamente se busca que no se vea frustrada la investigación en el futuro.

Asimismo, y más allá de la importancia que podría llegar a tener este tipo de medida en la sociedad actual, al día de hoy, muchos lugares no la tienen regulada. Un claro ejemplo es la falta de regulación en el ámbito de la Ciudad Autónoma de Buenos Aires.

Un intento fallido de regulación existió en el frustrado Proyecto del Código procesal Penal de la Nación en el año 2007. Éste, en su artículo 181, regulaba la mentada medida de la siguiente manera "el juez podrá ordenar, a requerimiento de parte y por auto fundado, el registro de un sistema informático o de parte de él, o de un medio de almacenamiento de datos informáticos o electrónicos con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación (…) aun antes de este requerimiento el fiscal podrá ordenar la conservación y protección de datos informáticos o electrónicos cuando existan razones para suponer que estos datos puedan ser perdidos o modificados. Esta medida podrá extenderse por un plazo de hasta noventa (90) días, a fin de obtener la orden judicial necesaria para su revelación".

Por último y toda vez que, como hemos adelantado, esta medida no se encuentra prevista en los códigos procesales, deberíamos analizar si se puede aplicar amparándonos en el principio de libertad probatoria. A mi entender, en este caso en particular, se podría implementar el principio de libertad probatoria toda vez que nos encontramos ante una

medida probatoria que no afecta a derechos y garantías de los ciudadanos toda vez que únicamente exige la conservación de la información y no su exhibición o divulgación.

B.1- Diferencias entre aseguramiento y retención de datos

Asegurar los datos significa conservar aquellos datos que ya se encuentran almacenados de alguna manera, protegiéndolos de cualquier interferencia que pudiera generar algún tipo de modificación en su calidad o condición actual.

Por otro lado, retener datos significa guardar el dato a partir del mismo momento en el cual está siendo generado, es decir implica retenerlo en el presente y guardarlo o mantenerlo para el futuro. Esta situación es aplicable a datos que no se encuentran almacenados.

Se podría entonces afirmar que la retención es el proceso a través del cual se almacenan los datos mientras que la conservación es aquella actividad que guarda el dato que ya se encontraba almacenado con anterioridad.

Por último, es importante resaltar que, en caso de que existiera la medida legislativa de carácter general de retención de datos, la medida de conservación de datos perdería utilidad, toda vez que los datos siempre se encontrarían resguardados. El problema es que la medida de retención de datos trae aparejados conflictos con garantías constitucionales por lo que, en principio, parecería que no va a ser regulada al corto plazo, motivo por el cual es importante que los estados regulen la medida de aseguramiento o, en su defecto, la empleen a través del principio de amplitud probatoria.

C- Aseguramiento y revelación parcial de datos de tráfico.

Esta medida probatoria se encuentra regulada en el artículo 17 de la Convención de Budapest y establece obligaciones específicas en relación a la conservación de los datos de tráfico así como una revelación rápida en relación a algunos datos de tráfico con la finalidad de identificar a los proveedores de servicios.

Tal como lo detalla el informe explicatorio de la Convención, es dable notar que la obtención de estos datos puede significar una pieza clave para poder determinar el origen o el destino de las comunicaciones realizadas, volviéndose un elemento crucial para la identificación de las personas que los han distribuido.

Existen distintas maneras de lograr esta conservación rápida, una de estas formas incluye la posibilidad de que, conforme explica el informe de la convención, las autoridades competentes presentaran rápidamente a cada proveedor del servicio órdenes individuales para esta conservación. Otra alternativa requiere una única orden general que se pudiera aplicar a todos los proveedores del servicio que posteriormente se determine que han participado en la transmisión de una comunicación determinada.

Por último, es importante poner en resalto que los datos de tráfico no son revelados a las autoridades encargadas de llevar a cabo el proceso cuando se envía una orden de conservación de datos, esto únicamente ocurrirá junto a otras medidas jurídicas tendientes a la revelación de estos datos.

Es por ello que las autoridades no tienen manera de saber si el proveedor de servicio al cual se le solicita la conservación posee todos los datos necesarios o si, por el contrario, otros proveedores lo tienen. En ese sentido, esta medida dispone que, aquel proveedor de servicio que reciba una orden de conservación de datos, deberá revelar rápidamente a las autoridades competentes una cantidad suficiente de datos de tráfico que les permita a las autoridades involucradas identificar a los proveedores de servicio y la vía por la cual se transmitió la comunicación. En esta ocasión las autoridades deberán especificar detalladamente el tipo de dato que deben ser revelados. En virtud de la información recabada será que las autoridades competentes podrán determinar si es o no necesario tomar una medida de conservación respecto de otros proveedores de servicio.

D- Orden de presentación

La orden de presentación se encuentra regulada en el artículo 18 de la Convención de Budapest. En este artículo se insta a las partes a que faculten a las autoridades competentes de cada Estado a que ordenen a determinada persona en su territorio a brindar determinados datos informáticos que tenga en su poder o a que ordene a determinado proveedor que entregue información relativa al abonado.

De la misma manera, puede ser definida como "la facultad de las autoridades competentes de ordenar a una persona que se encuentre en su territorio que comunique determinados datos informáticos o datos relativos a los abonados que obren en su poder o estén bajo su control, almacenados en un sistema informático o en un dispositivo de

almacenamiento de datos"[21]. Esta medida insta a que se presenten los datos que se encuentran almacenados y a los ya existentes, no así aquellos que aún no han sido generados (los datos relativos al tráfico o los datos relativos al contenido con respecto a comunicaciones futuras).

Es muy importante señalar la importancia de que estos datos se encuentren bajo el poder o control de la entidad a quien se le solicita la mentada medida. A su vez, es un requisito indispensable que los mismos estén almacenados en un dispositivo informático y que se trate de datos del pasado, ya que los datos del futuro son competencia de otra norma procesal, aquella referente a la intervención de datos de tráfico o contenido.

Es decir, esta medida únicamente se refiere a datos informáticos que se encuentren almacenados o existentes, específicamente a los que estén en poder de determinada persona o proveedor de servicios. En concreto, la orden de presentación se podrá solicitar sobre datos informáticos que se encuentren en pode" o bajo el control de determinada persona o proveedor de servicio. La expresión obran en su poder o estén bajo su control "se refiere a la posesión física de los datos en cuestión en el territorio de la Parte que imparta la orden y también a situaciones en las cuales la persona no tenga la posesión física de los datos que deben presentarse, pero que dicha persona pueda, no obstante, controlar libremente la presentación de los mismos desde dentro del territorio de la Parte que imparte la orden … al mismo tiempo, la mera capacidad técnica para acceder remotamente a datos almacenados (por ejemplo, la capacidad que tiene un usuario para acceder a distancia a través de un enlace de red a datos almacenados que no están bajo su control legítimo) no constituye necesariamente "control" con arreglo al significado de esta disposición"[22]. A su vez, las partes deben tener la facultad de ordenar a determinado proveedor de servicios a que comunique los datos que obren en su poder o estén bajo su control relativos a los abonados.

El informe explicativo alienta a los Estados parte a que, en lugar de aplicar de manera sistemática medidas coercitivas como lo puede ser el registro o confiscación de datos, incluyan en su derecho interno distintas facultades de investigación que brinden medios menos intrusivos a los derechos y garantías de los seres humanos a fin de obtener información relevante en el proceso, es decir medios más "flexibles" para poder asegurar los fines del proceso.

[21]Definición dada por los integrantes del Comité de Ministros del Consejo de Europa en el Informe explicativo del Convenio sobre Ciberdelincuencia aprobado el 8 de noviembre de 2001 -ver Acápite 178-.
[22]Explicación brindada por los integrantes del Comité de Ministros del Consejo de Europa en el Informe explicativo del Convenio sobre Ciberdelincuencia aprobado el 8 de noviembre de 2001 -ver Acápite 173-

Ahora bien, es hora de preguntarnos qué ocurre en nuestro ordenamiento procesal. A modo de ejemplo, el Código Procesal Penal de la Ciudad de Buenos Aires prevé en el párrafo tercero del art. 119 que "El/la Fiscal podrá ordenar, cuando fuere oportuno, la presentación de los objetos o documentos a que se refiere este artículo, con excepción de los elementos citados en el art. 13 inc. 8 de la Constitución de la Ciudad Autónoma de Buenos Aires".

A su vez, "Concordantes con el texto Nacional y de la Ciudad de Buenos Aires son el de la Provincia de Buenos Aires -art. 227 [actual artículo 232]-, de Chubut -art. 178 Párrafo 2do.-, de Córdoba -art. 211- y de Neuquén -art. 147- entre otros, y la única diferencia entre ellos pareciera estar dada por la sola circunstancia que en algunos se encuentra en una norma específica referida a la orden de presentación y en otros está inserta en el propio artículo donde se regula la medida de prueba del secuestro, ubicación esta última que tiene explicación en dos hechos, el primero dado porque habitualmente se la consideraba como una medida de coerción procesal accesoria, ya que precisamente posibilitaba la realización del primero al que se lo consideraba como medida principal y el segundo, consistente en que se la estimaba a su vez subsidiaria, ya que la entendían algunos autores como una alternativa que evitaba precisamente la ejecución del secuestro"[23].

Lo importante es destacar la necesidad imperante de una modificación a nivel legislativo que permita regular la orden de presentación como una medida autónoma y, a su vez, adaptadas para el mundo digital.

E- Registro y confiscación de datos informáticos almacenados

Esta medida se encuentra regulada en el artículo 19 de la Convención de Budapest. Tanto el registro como el secuestro de los datos informáticos, han cobrado mucha relevancia en esta "nueva era del derecho procesal penal". Ahora bien, es imperioso aclarar que el mencionado Convenio no establece la manera en que se permitirá o llevará a cabo la extensión de un registro, sino que ello va a depender del derecho interno de cada país.

En un primer análisis, si se quiere "lógico", podríamos decir que, para el registro y confiscación de datos informáticos, es necesario contar con el "soporte físico" en el que se encuentran almacenados los datos a confiscar. Es decir que el registro y confiscación de datos se efectúa sobre dispositivos electrónicos que deben haber sido incorporados con anterioridad

[23]Véase, COLEFF, "La orden de presentación en el derecho procesal penal Argentino. Necesidad de su reforma" en DUPUY (dir.)/ KIEFER (cord.) *Cibercrimen. Aspectos del Derecho penal y procesal penal,Buenos Aires, BdeF, 2017, cap III.*

al procedimiento. Entonces, para que estas medidas probatorias sean válidas, los dispositivos electrónicos deben haber sido incorporados previa y legítimamente al proceso en cuestión.

Las mentadas medidas probatorias se podrían efectuar tanto sobre el soporte físico en sí mismo, como sobre una copia forense de los datos. Esta copia se realiza sobre el soporte original, respetando todas las medidas necesarias para que dicha copia sea legítima y, así lo sea también, la información que se obtenga de ella.

En concreto, se podrían distinguir dos etapas dentro del registro y confiscación de datos informáticos. En primer lugar, el secuestro del soporte físico y luego la búsqueda de los datos mediante técnicas informáticas que se apliquen sobre los mentados dispositivos.

Así, dentro de este marco existiría una firma distinción entre:

A.- Los requisitos, que actualmente ya se encuentran actualmente regulados en los códigos procesales - por ejemplo, de la Ciudad Autónoma de Buenos Aires (Artículos. 114 y siguientes., CPPCABA)- para llevar a cabo el allanamiento/ requisa y posterior secuestro del "soporte físico" sobre el cual se va a trabajar y,

B.- los requisitos "tácitos" para llevar a cabo las copias forenses y los que refieren al registro y secuestro de los datos informáticos.

Es importante destacar que esta medida "Se aplica a los datos informáticos almacenados. Respecto de esto, se plantea la cuestión de si un mensaje de correo electrónico no abierto que se encuentra en el buzón de entrada de mensajes de un proveedor de Internet hasta que el destinatario lo descargue a su sistema informático, debe considerarse datos informáticos almacenados, o datos en proceso de transferencia. Conforme a las leyes de algunas Partes, ese mensaje de correo electrónico es parte de una comunicación y, por consiguiente, su contenido sólo puede obtenerse aplicando la facultad de interceptación; por el contrario, otros sistemas jurídicos consideran dicho mensaje como datos almacenados a los que corresponde aplicar el Artículo 19. Por consiguiente, las Partes deberían analizar su legislación respecto de esta cuestión para determinar lo que es apropiado con arreglo a sus respectivos ordenamientos jurídicos"[24].

En concreto, la pregunta que debemos efectuarnos es si la utilización de estas nuevas tecnologías en el marco del procedimiento penal a fin de obtener evidencia resulta o

[24]Explicación brindada por los integrantes del Comité de Ministros del Consejo de Europa en el Informe explicativo del Convenio sobre Ciberdelincuencia aprobado el 8 de noviembre de 2001 -ver Acápite 190-

no admisibles en el proceso penal de la Ciudad Autónoma de Buenos Aires, teniendo en consideración dos puntos fundamentales: el marco constitucional y las normas procesales.

A su vez, hay que analizar lo que ocurre con la teoría norteamericana del *plain view* (hallazgo a simple vista o inevitable), es decir la teoría por la cual si en el marco de, por ejemplo, un allanamiento el personal autorizado se topa a simple vista con prueba o rastros de otros delitos, tiene el deber de denunciar y preservar aquella prueba.

En ese sentido, es dable observar que, en materia de allanamientos de objeto físico, existe acuerdo jurisprudencial y doctrinario en las diferentes aristas que se pueden dar de esta teoría. Pero, en el ámbito informático, es distinto y no existe acuerdo sobre la postura que hay que tomar respecto de esta toda vez que todos los datos que la persona maneja están en un mismo dispositivo pero en un compartimiento distinto, y gran parte de las aplicaciones funcionan con búsquedas automáticas.

Por último, se debe tener presente que es imposible intentar asimilar una medida de registro y secuestro informático al registro y secuestro de elementos físicos, toda vez que las diferencias entre las cosas físicas y los datos informáticos delimita la necesidad de una normativa que regule de manera diferenciada ambas medidas. En concreto la aplicación analógica de normas delimitadas para el secuestro de objeto físico al secuestro de datos informáticos es insuficiente tanto para la investigación, como así también para una protección adecuada de las garantías de los individuos sometidos al proceso.

F- Desencriptación compulsiva de datos

Si bien las medidas que hemos analizado en este trabajo son medidas básicas y existen otras medidas que, por cuestión de extensión no vamos a analizar, entre ellas el acceso transfronterizo de datos, el allanamiento remoto, entre otros, si vale la pena hacer un breve análisis de la desencriptación compulsiva de datos como un subtema dentro de la problemática del registro y secuestro de datos. Esa problemática se observa a raíz de que en numerosos allanamientos se secuestran dispositivos que, por sus características propias no se puede acceder a ellos porque poseen un sistema de encriptación.

En la actualidad, las personas habitualmente se encuentran en contacto con la tecnología a través de dispositivos electrónicos –celulares, computadoras, diarios electrónicos, etc.-, y que, a su vez, estos dispositivos cuentan con un sinfín de

información personal la que, en caso de encontrarnos en el marco de un procedimiento penal, puede llegar a ser muy valiosa.

Con el avance de la tecnología, se han creado nuevos sistemas a través de los que esos dispositivos pueden encontrarse cifrados de distintas maneras, con contraseñas, huellas dactilares o identificación biométrica. Según la Real Academia Española cifrado significa: "Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger un dispositivo". que un dispositivo cifrado atravesó un proceso a través del cual "se vuelven ilegibles datos o información que se encuentre almacenada en un dispositivo electrónico, a la que solamente se podrá acceder con una contraseña. Se trata de una medida de seguridad que permitiría mantener una comunicación en privado o, al menos, mantenerla más segura"[25].

Es por ello que los operadores del sistema judicial pueden afrontar grandes desafíos cuando se encuentran en una situación en la cual deben acceder a estos dispositivos cifrados, Especialmente en ocasiones en las que la persona involucrada no se encuentra dispuesta a brindar datos de su contraseña, huella digital o datos biométricos.

Ahora bien, ante la negativa de la persona sometida al proceso ¿se le puede exigir que brinde estos datos, o estaríamos violando el derecho que esta tiene a no declarar contra si misma? y, en caso de estar obligando a esta persona a autoincriminarse, ¿No sería nula toda la prueba obtenida del dispositivo electrónico en cuestión?

El derecho a no declarar contra uno mismo, surge como garantía consagrada en el artículo 18 de la Constitucional Nacional, el cual reza, en lo que aquí interesa: "nadie puede ser obligado a declarar contra sí mismo". A su vez, esta misma garantía la encontramos contenida en el artículo 8.2 inciso g) de la Convención Americana de Derechos Humanos y en el artículo 14. 2 inciso g) del Pacto Internacional de Derechos Civiles y Políticos (ambos con jerarquía constitucional vía 75 inc. 22 C.N.); cuya

[25]PORTILLO, Víctor Hugo/ MATTEO Juan Manuel, "Autoincriminación y nuevas tecnologías" en *Sistema penal e informática,* vol. II, 2021, p. 178 y sig.

inobservancia no solo llevaría a la nulidad de lo actuado, sino que, a su vez, podría acarrear como consecuencia responsabilidad ante la comunidad internacional.

Aquí el problema recae en que el uso de la evidencia digital es cada día más imprescindible en el marco de las investigaciones penales. Entonces, ante la falta de regulación que nos impide efectuar un proceso penal respetuoso de las garantías constitucionales, podríamos decir que se le suma un nuevo problema ¿Qué hacer con esa valiosa información que se encuentra cifrada?, ¿acaso se puede seguir avanzando sobre las garantías del imputado ante la inexistencia de un marco regulatorio?

Ahora bien, el principio de libertad probatoria, como es sabido, encuentra límites, algunos establecidos expresamente en los códigos y otros que surgen de principios y garantías. Entonces, para resolver las cuestiones acerca de esta medida en particular habría que analizar si se puede o no aplicar el principio de libertad probatoria. Ante esto, encuentro dos posibles respuestas.

Una visión más estricta, desde la cual no se puede emplear un medio probatorio no regulado que signifique una coerción para los derechos y garantías del imputado, plantea que no es posible acceder a esta información cifrada sin caer en una nulidad. Una segunda postura, un poco menos rígida, podría establecer que, para el caso de que el medio no esté regulado expresamente, pero si exista una medida de prueba de similar característica y de mayor injerencia que si este regulada, se podría emplear.

IV.- ¿Qué pasa en el resto de los países?

A Convención de Budapest

Fue en virtud del desarrollo de las nuevas tecnologías que en el año 1996 el Comité Europeo para los problemas criminales decidió establecer un comité de expertos que se encargaran específicamente de los delitos informáticos (CDPC).

A su vez, el Comité de Ministros estableció en el año 1997 el nuevo comité denominado "Comité de Expertos en la Delincuencia del Ciberespacio" (PC-CY), el que se encargó de efectuar las negociaciones en relación a un proyecto internacional sobre la ciberdelincuencia. Los Ministros de Justicia europeos respaldaron todas las negociaciones a fin de lograr que las disposiciones internas de cada país en el ámbito del Derecho penal fuesen lo más parecidas entre si y, a su vez, de permitir el uso de medios eficaces de investigación en cuanto a los delitos informáticos. Sumado a ello reconocía la necesidad de contar con un sistema de cooperación internacional rápida y eficiente, que tuviera en cuenta debidamente las necesidades específicas que lleva aparejada la lucha contra la ciberdelincuencia.

Finalmente, en el año 2001, específicamente el día 8 de noviembre fue aprobado el Convenio sobre la ciberdelincuencia junto a su informe explicativo por el Comité de Ministros del Consejo de Europa. En ese mismo sentido, el mentado Convenio fue abierto a la firma en Budapest el día 23 de noviembre de ese mismo año.

Es importante resaltar que este tuvo en miras tres grandes objetivos, primero buscó armonizar los elementos de los delitos conforme al derecho penal de fondo de cada país y de las disposiciones conexas en materia de delitos informáticos, segundo buscó establecer, según el derecho procesal penal de cada país parte, los poderes necesarios para la investigación y el procesamiento de los delitos informáticos como así también de otro tipo de delitos cometidos a través del uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico, y tercero, fijar un

régimen rápido y eficaz de cooperación internacional 3) establecer un régimen rápido y eficaz de cooperación internacional[26].

B- El caso de España

En España, por Real Decreto de 14 de septiembre de 1882 se aprobó la Ley de Enjuiciamiento Criminal a través de la cual, a través de distintas normas legales, se regulan las actuaciones judiciales que hacen al proceso penal. La misma ha sufrido diversas modificaciones, entre ellas, la ocurrida luego de adherir a la convención de Budapest, en virtud de las obligaciones asumidas por el país a fin de incorporar normas que regulen la evidencia digital[27].

La mentada ley buscó proteger a los ciudadanos de las diferentes formas de afectación a las garantías constitucionales que las medidas coercitivas tecnológicas pueden significar. A continuación, y a modo ilustrativo, reflejaré alguna de las incorporaciones en materia de evidencia digital.

En primer lugar, me remitiré al Artículo 588 *bis* a, el cual establece disposiciones comunes aplicables a todas las medidas, entre ellas, a la necesidad de una autorización judicial dictada por autoridad competente y sujeta a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. A su vez, esta debe encontrarse relacionada con la investigación de un delito en concreto, es decir no a fin de prevenir o descubrir delitos. En relación al principio de excepcionalidad y necesidad, aclara que estas medidas podrán emplearse siempre que no existan a disposición de los órganos de persecución penal medidas menos gravosas para los derechos fundamentales del investigado y sean igualmente útiles para el esclarecimiento del hecho o cuando el descubrimiento del hecho o su autoría, paradero o localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

También, podemos mencionar al Artículo 588 *ter* a, el cual regula la interceptación de las comunicaciones telefónicas y telemáticas. Éste limita la medida para ocasiones en las que la investigación tenga por objeto alguno de los distintos

[26]Véase, Convenio sobre la ciberdelincuencia (STE núm. 185) Informe explicativo, p.5.
[27]Ley Orgánica 13/2015, del 5 de octubre, de 2015 modificación de la Ley de Enjuiciamiento Criminal, publicada en el Boletín Oficial del Estado BOE, 239, 6 de octubre del 2015.

delitos contenidos en el artículo 579.1 de esa Ley, delitos cometidos a través de instrumentos informáticos o de cualquier tecnología de la información o la comunicación o servicio de comunicación.

A, su vez el Artículo 588 *ter* j regula la orden de presentación al referir que aquellos datos electrónicos conservados por los prestadores de servicios o particulares, en cumplimiento con la normativa sobre retención de datos –ley de retención de datos del año 2007-, o por propia iniciativa y que estén vinculados a procesos de comunicación únicamente serán cedidos con autorización judicial y, si esos datos son indispensables para la investigación, se requerirá al juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores.

Entre los Artículos 588 *ter* k hasta ter m encontramos medidas relativas a la preservación de datos de tráfico. En ese sentido, a modo de ejemplo, el Artículo 588 ter k expone que, cuando los agentes de la policía judicial, en el ejercicio de sus funciones de prevención y descubrimiento de delitos en internet, tengan acceso a una dirección IP la cual se estuviera empleando para algún delito y, no constara la identificación y localización del equipo o del dispositivo de conectividad, ni datos de identificación personal, podrán solicitar al juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el Artículo 588 ter e la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

El Artículo 588 *sexties* A, regula lo que hace al registro datos informáticos. En esa ocasión, el Juez competente, a la hora de efectuar una resolución para permitir un registro domiciliario donde sea previsible la necesidad de aprehensión de ordenadores o algún tipo de dispositivo informático, deberá extender su razonamiento a la justificación de las distintas razones que legitiman al acceso de los agentes facultados a la información que contengan los mencionados dispositivos. La incautación del dispositivo informático practicada durante la diligencia del registro domiciliario no autoriza al acceso a su contenido.

Por último, haré mención a la medida contenida en el Artículo 588 *octies* relativa a la conservación de datos. Esta medida enuncia que tanto el Ministerio Público Fiscal como la Policía judicial podrán requerir a cualquier persona, física o jurídica, la conservación y protección de datos informáticos concretos incluidos en un sistema

informático de almacenamiento que esté a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión. Estos serán conservados por un máximo de noventa días prorrogables una única vez.

C- El caso de Brasil

Para comenzar, debo advertir que, debido a cuestiones de extensión del presente trabajo, me limitaré a exponer tres leyes relevantes que reflejan el desarrollo obtenido en materia de evidencia digital.

En primer lugar, se encuentra la Ley n° 9296 del 24 de Julio de 1996, la cual regula el inciso XII, parte final del artículo cinco de la Constitución Federal, el cual habla acerca de la inviolabilidad del secreto de la correspondencia, de las comunicaciones telegráficas, de la data y comunicaciones telefónicas y sus límites. Estos están dados por la necesidad de una orden de autoridad judicial, emanada de autoridad competente, en situaciones y formas estipuladas por ley y para los fines de investigación criminal o búsqueda de hechos en la fase de acusación criminal[28].

La mentada Ley regula no solo la interceptación de comunicaciones telefónicas, de flujo de comunicaciones en sistemas informáticos y telemáticos, sino que también hace referencia a la regulación de la captura ambiental de señales electromagnéticas, ópticas o acústicas para investigación o instrucción penal.

En referencia a la interceptación de las comunicaciones telefónicas y de sistemas informáticos y telemáticos, refiere que únicamente se podrán realizar las mentadas medidas por orden de Juez competente y bajo secreto de justicia. A su vez, limita la aplicación de estas medidas, prohibiéndolas cuando no exista evidencia razonable a fin de establecer la autoría o la participación, cuando la prueba pueda efectuarse por otros medios y cuando el hecho sea una infracción penal la que, como máximo, esté penada con prisión preventiva.

Estas medidas pueden ser solicitadas de oficio por el juez o a solicitud de la autoridad policial o del Ministerio Público Fiscal, pero siempre debe demostrarse que es necesaria para la investigación. Por último regula la manera en la que la medida debe llevarse a cabo.

[28]Inciso XII art. 5 de la Constitución Federal: *"El secreto de la correspondencia, de las comunicaciones telegráficas, de la data y comunicaciones telefónicas es inviolable, a excepción, en el último caso, por orden judicial, en las situaciones y en la forma prescrita por ley para fines de investigación criminal o búsqueda de hechos en la fase de acusación criminal"*.

Por otra parte, en lo que hace a las medidas relativas a la captura ambiental de señales electromagnéticas ópticas o acústicas, hace hincapié en que únicamente podrán efectuarse con autorización del juez competente a solicitud de autoridad policial o del Ministerio público. Éstas únicamente pueden aplicarse a aquellas situaciones en los que la prueba no puede realizarse por otros medios disponibles e igualmente eficaces y para cuando existan elementos probatorios razonables en materia de autoría y participación para infracciones penales cuyas penas máximas sean superiores a cuatro años de prisión o en infracciones penales conexas. Asimismo, debe encontrarse descripto lo que hace al detalle de lugar y forma de instalación del dispositivo de captura ambiental.

Si bien en esta Ley fue vetada la propuesta que permitía la instalación del captador ambiental mediante operativo policial encubierto o de noche, con excepción de la casa, éste fue finalmente incluido por la Ley N ° 13.964, de 2019. Por otro lado, la propia Ley limita la financiación ambiental al plazo de quince días, renovable por decisión judicial por períodos iguales, siempre que se acredita la indispensabilidad de la prueba y cuando se presenta actividad delictiva permanente, habitual o continuada.

Por último, la Ley es clara en cuanto a que aquellas grabaciones que no fueran de interés para la investigación quedarían, por orden judicial, inutilizadas.

Otra Ley de interés para la presente investigación es la n° 12850 del 2 de agosto del 2013 que, entre otras materias, en su capítulo segundo “Investigación y medios de obtención de prueba”, efectúa una enumeración de aquellas medidas probatorias que considera permitidas en el marco del proceso penal. Entre estas se incluye la captura ambiental de señales electromagnéticas, ópticas o acústicas, el acceso a registros de llamadas telefónicas y telemáticas, y la interceptación de comunicaciones telefónicas y telemáticas, en los términos de la legislación específica.

En su sección III, relativa a la “infiltración de agentes”, en su Artículo 10 A incluye la figura del policía virtual infiltrado en internet, a fin de poder investigar los delitos previstos en la mentada Ley siempre que se demuestre que sea necesario y, a su vez, se indique el alcance de las funciones de los policías, los nombres de los investigados y, en caso de ser posible, los datos de conexión o registro que permitan la identificación de las personas en cuestión. A su vez, brinda una definición para los alcances de esa Ley de los datos de conexión y datos registro.

También se encarga de limitar la mentada medida y se vuelve a hacer hincapié en que únicamente se podrá realizar toda vez que no pueda ser aportada la prueba necesaria por otros medios disponibles. Por último, brinda un plazo temporal por el cual se permitirá la infiltración, en este caso seis meses, renovables mediante orden judicial motivada la que no puede exceder los setecientos veinte días.

Es importante resaltar que de la misma Ley emana que toda aquella prueba que sea obtenida sin dar observancia a las limitaciones brindadas por aquella será nula y sin valor y, por lo tanto, el policía informático que se exceda en su labor deberá responder por los excesos efectuados. Por último, refiere que la prueba obtenida legítimamente será confidencial.

En última instancia, se encuentra la Ley N° 12965 del 23 de abril del 2014 la cual establece principios, garantías, derechos y deberes para el uso de internet en Brasil. Al comienzo efectúa una enumeración de principios en los cuales se basa el uso de internet, entre los cuales se encuentran, a modo de ejemplo, la garantía de libertad de expresión, también la protección a la privacidad, a los datos personales, entre otros.

A su vez, en su capítulo segundo enumera los derechos y garantías de los usuarios de internet, entre los que se encuentran, la inviolabilidad de la intimidad de la vida privada, su protección e indemnización por el daño material o moral resultante de su violación, la inviolabilidad y secreto del flujo de sus comunicaciones a través de Internet, salvo orden judicial, de conformidad con la Ley, inviolabilidad y confidencialidad de sus comunicaciones privadas almacenadas, excepto por orden judicial; no facilitar a terceros sus datos personales, incluidos registros de conexión y acceso a aplicaciones de internet, salvo consentimiento libre, expreso e informado o en los casos previstos por lay, entre otros.

Establece fehacientemente que la garantía del derecho a la intimidad y libertad de expresión en las comunicaciones es condición para el ejercicio pleno de acceso a internet y, en ese sentido, que serán nulas y sin efecto cláusulas que impliquen una ofensa a la inviolabilidad y confidencialidad de las comunicaciones privadas.

La sección segunda “Protección de registro, datos personales y comunicaciones privadas” establece claramente que la custodia y disponibilidad de los registros de conexión y acceso a las aplicaciones de internet, como los datos personales

y el contenido de las comunicaciones privadas, deben cumplir con la preservación de la intimidad, la vida privada, el honor y la imagen de las partes implicadas.

A su vez, en la Subsección I "De la conservación de registros de conexión", establece que, en la provisión de conexión a internet, será deber de los administradores del sistema autónomo respectivo mantener los registros de conexión bajo confidencialidad en un ambiente controlado y de seguridad por el término de un año, período que se podrá extender a solicitud de la autoridad policial o administrativa o el ministerio público, la cual deberá contar con orden judicial.

Por último, en la Subsección III "Mantenimiento de registros de acceso a las aplicaciones de internet en el suministro de aplicaciones" enuncia que los prestadores constituidos en forma de persona jurídica que lleve a cabo la actividad de manera organizada, profesional y con fines económicos, deberá mantener los respectivos registros de acceso a las distintas aplicaciones de internet bajo confidencialidad de forma controlada por un período de seis meses. A su vez, con una orden judicial, la autoridad policial o administrativa o el Ministerio Público podrán solicitar provisionalmente a cualquier proveedor de aplicaciones de internet que se conserven los registros de acceso a las aplicaciones de internet, incluso por un período superior al previsto.

D- El caso de Perú

En lo referente a Perú existen diversas legislaciones que regulan la materia, entre ellas y a modo de enunciar algunos ejemplos, podemos observar la Ley N° 27697 del año 2002 que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en casos excepcionales. La Ley se limita a determinado tipo de delitos considerados especialmente graves, entre ellos, el secuestro, la trata de personas, la pornografía infantil, entre otros.

En lo que hace el derecho penal de fondo, la Ley N° 30096 del año 2013 regula delitos informáticos, entre los que se encuentra el acceso ilícito, el atentado contra la integridad de datos informáticos, el atentado contra la integridad de sistemas informáticos, delitos informáticos contra la indemnidad y libertad sexual, entre otros.

A su vez, el Decreto Legislativo n° 1182 del año 2015 regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y

geolocalización de equipos de comunicación. Su finalidad principal, conforme reza su artículo primero, es el "(…) fortalecer las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado a través del uso de tecnologías de la información y comunicaciones por parte de la Policía Nacional del Perú (…)".

En ese sentido, limita el acceso inmediato a los datos de localización o geolocalización de teléfonos y dispositivos electrónicos para tres tipos de casos. Primero, cuando se trate de un flagrante delito; segundo, cuando el delito sea sancionado con una pena superior a los cuatro años de privación de la libertad; y, por último, cuando el acceso a los datos constituya un medio necesario para la investigación.

A su vez, aclara que esta normativa únicamente se aplica a datos de localización o geolocalización lo que significa que queda excluido expresamente cualquier tipo de intervención de las telecomunicaciones.

En sus disposiciones finales regula la conservación de los datos que derivan de las telecomunicaciones, imponiendo la obligación a los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas de conservar los datos derivados de las telecomunicaciones durante los primeros doce meses en sistemas informáticos que permita su consulta y entrega en línea y en tiempo real. A su vez, una vez concluido ese plazo, obliga a conservar los datos por veinticuatro meses adicionales.

V.- ¿Qué sucede en Argentina?

Como hemos adelantado anteriormente, en general, el pronunciado atraso en nuestro sistema procesal ha llevado a los jueces muchas veces a llenar esos vacíos legales con la aplicación analógica de las normas previstas para lo relativo a la obtención de la prueba física. Es importante observar que, en el caso de nuestro país, las leyes procesales penales, usualmente no tienen dispositivos dedicados exclusivamente a lo que hace a la regulación de las medidas probatorias para la incorporación de evidencia digital al proceso y únicamente se cuenta con normas procesales para la incorporación de evidencia física o normas procesales que autorizan en trazos generales la interceptación de las comunicaciones y el secuestro de correspondencia o papeles privados.

Esta situación ha llevado a que, en variadas ocasiones, los auxiliares de justicia hayan empleado medidas de pruebas no regladas en algunas investigaciones, con conocimiento de la autoridad judicial y, en ese sentido, aplicando analógicamente normativa relativa a medidas probatorias reguladas para la evidencia física.

Uno de los primeros antecedentes que podemos observar en el país es el proyecto de Ley de reforma puntual del código procesal penal de la nación, elaborado por la Comisión Técnica Asesora en Materia de Cibercrimen. Este proyecto, presentado a mediados del mes de octubre del año 2013, buscaba modificar el Título de medios de prueba. Su objetivo concreto era sumar normas procesales relativas a lo que hace al tratamiento de las pruebas digitales y, de esta manera, contribuir a la adecuación del sistema procesal penal a los postulados de la Convención de Budapest.

Entre otras normas y, más allá de que la mentada Convención no lo preveía, buscaron regular el acceso remoto a sistemas informáticos como una modalidad especial de allanamiento. En ese sentido, se agregaba una habilitación legal para registrar los dispositivos informáticos encontrados en el marco de un allanamiento físico. Es decir, requería, en primer

lugar, un allanamiento para la obtención del dispositivo físico para, luego, permitir de manera remota la obtención de la información digital.

A su vez, el artículo tercero proponía una habilitación expresa a la utilización de las técnicas de acceso remoto cuando "existieren motivos para presumir que un dispositivo de almacenamiento informático contiene datos relativos a la investigación y fuera posible el registro de tal dispositivo por medios técnicos y en forma remota… su objeto deberá estar precisamente detallado, bajo pena de nulidad ".

En ese orden de ideas encontramos también el Código Procesal Penal de la Provincia de Neuquén (CPPN Ley 2784 del año 2011) en su capítulo tercero, artículo 153, regula la información digital de la siguiente manera: "(…) Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, **se procederá a su secuestro, y de no ser posible, se obtendrá una copia**. O podrá **ordenarse la conservación de los datos** contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las **medidas necesarias para mantenerla en secreto**. También podrá disponerse el **registro del dispositivo por medios técnicos y en forma remota**. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá **requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos**. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos"- el destacado me pertenece-.

En definitiva, el CPPN habilita el registro y secuestro de datos en equipos informáticos para:

a) Equipos informáticos hallados en el marco de un allanamiento, es decir la obtención de datos desde el dispositivo físico.
b) Registros remotos a distancia.

A su vez, autoriza la conservación de datos y la entrega de información a las empresas que prestan servicios por vía electrónica.

En el mismo cuerpo normativo se observa observar el artículo 150, el cual esboza: "Podrá ordenarse la obtención, aun en tiempo real, de los datos de tráfico de las

comunicaciones transmitidas por un sistema informático y también el contenido de las mismas. La intervención de comunicaciones tendrá carácter excepcional y podrá renovarse cada quince (15) días, expresando los motivos que justifican la extensión del plazo. Las prórrogas no podrán superar los noventa (90) días"

Asimismo, existió la propuesta de reforma al Código Procesal Penal de la Nación, (Ley n° 27.063 en el año 2016). Aquí, el PEN efectuó un proyecto para modificar parcialmente al texto original de la norma. En concreto, buscaba agregar un apartado acerca de "medios especiales de investigación". En el marco de este nuevo título, a modo de ejemplo, incorpora un artículo a la vigilancia remota de equipos informáticos, es decir, habilita el uso de programas informáticos para acceso a los distintos sistemas informáticas de las personas investigadas.

Sumado a ello, deja a arbitrio del juez el análisis de razonabilidad de las medidas a adoptarse, sobretodo en estos casos de especial gravedad. Aquí, conforme resalta Salt, se puede efectuar una crítica al mentado proyecto toda vez que termina dejando a la valoración judicial cuáles son los supuestos de delitos concretos de especial gravedad, a fin de efectuar la habilitación legal.

En conclusión, y considerando los pocos ejemplos traídos a colación en virtud de la extensión del presente trabajo, se puede observar que lo que hace a la regulación procesal penal en el país es bastante escasa. En virtud de ello, entiendo que se requerirá de una gran labor legislativa a fin de poder regular estos "vacíos" legales que dejan lugar a la aplicación de principios como el de libertad probatoria a costa de la vulneración de derechos fundamentales de los ciudadanos.

VI.- Conclusión

En primer lugar, y como he adelantado anteriormente, en la mayoría de los códigos de procedimiento penal del país no existe normativa que habilite de manera expresa el empleo de determinados medios de coerción a fin de incorporar evidencia digital al proceso penal. Esta falta de regulación lleva a un pronunciado conflicto entre los derechos de los individuos sometidos al proceso penal y los mecanismos –aún no regulados- de los que se vale el Estado para recabar información. La falta de medidas legislativas, se traduce en una grave injerencia por parte del estado en el ámbito de los derechos de las personas, violando así garantías y derechos de la persona sometida al proceso.

Estas nuevas medidas probatorias, como no se encuentran reguladas, han sido empleadas de la mano del principio de libertad probatoria, principio que no debería aplicarse de manera ilimitada y mucho menos a medidas que se traducen en una coerción estatal sobre los derechos del imputado. Ya hemos enunciado que el principio de libertad probatoria no solo no debe aplicarse a medidas coercitivas, sino que también hay que analizar, en el caso en concreto, si se puede emplear la analogía y, a su vez, si esa aplicación analógica es en perjuicio del imputado o no. En conclusión, entiendo que el empleo de estas técnicas que actualmente no se encuentran reguladas únicamente llevaría a la imposibilidad de introducir válidamente la información recabada a través de estas al proceso penal.

Ahora bien, considero que una postura tan rígida respecto a estas nuevas medidas probatorias llevaría a la imposibilidad de continuar numerosas investigaciones penales. Es por eso que, ante la situación actual, se pueden tomar dos posturas: o nos

centramos en una mirada estricta en la que toda medida de prueba que signifique una coerción estatal y no esté regulada sea considerada inválida, u optamos por una mirada más conciliadora, que permita aplicar analógicamente estas medidas, siempre y cuando en el ordenamiento procesal exista otra medida coercitiva más invasiva.

Entonces, ¿cómo hacemos para superar estas dificultades? En primer lugar, y como he expuesto a lo largo del presente trabajo, creo necesaria una regulación de estas nuevas medidas probatorias con la finalidad de que, por un lado, se respeten los derechos y garantías de los imputados y, por otro, pueda llevarse a delante un proceso penal legítimo.

A su vez, no escapa de mi conocimiento que estas medidas injieren de manera aguda en los derechos fundamentales de las personas, como puede ser el derecho a su vida privada, a su intimidad, a la privacidad de los datos electrónicos motivo por el cual su regulación debe ser exhaustiva. Es decir, bajo el entendimiento de que los ciudadanos deben encontrarse resguardados de las injerencias injustificadas por parte del Estado en su vida privada y que, por otro lado, los órganos encargados de la persecución penal deben tener a su alcance las medidas necesarias para efectuar de manera correcta la investigación llegamos a la conclusión de que no cualquier norma va a satisfacer las condiciones de legitimidad necesaria.

En ese sentido, al hablar de los derechos de los ciudadanos y su regulación, el art. 28 de la Constitución Nacional reza: "(…) los principios, garantías y derechos reconocidos en los anteriores artículos, no podrán ser alterados por las leyes que reglamenten su ejercicio (…)". Eso se traduce en que aquella Ley destinada a regular un derecho no puede modificarlo sustancialmente.

En definitiva, se deberá desarrollar una normativa orientada a encontrar el equilibrio entre los derechos de los ciudadanos, específicamente el derecho a la intimidad a la vida privada, y al mismo tiempo, a la efectividad de las investigaciones efectuadas por parte del estado en esta nueva "era digital". Habrá que buscar la forma de que, en virtud de los principios de necesidad y proporcionalidad, se efectúen distintas normas que habiliten el accionar del Estado, teniendo en consideración el grado de injerencia estatal que la mentada normativa requeriría.

En conclusión, resalto la importancia de estos nuevos medios de investigación e incluso creo que, en un futuro no muy lejano, pasarán a ser los

protagonistas de las investigaciones penales. Es por ello que lejos me encuentro de descartar, sin más, su implementación, mas bien enfatizo la necesidad imperante de una minuciosa regulación.

VII.- Bibliografía

BRUZZONE, Gustavo A., Homenaje al profesor Julio B. J. Maier estudios sobre justicis penal *La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso pena"*, Buenos Aires, Editores del Puerto, 2005.

COLEFF, Iván "La orden de presentación en el derecho procesal penal Argentino. Necesidad de su reforma" en DUPUY Daniela (dir.)/ KIEFER Mariana (cord.) *Cibercrimen. Aspectos del Derecho penal y procesal penal,* , Buenos Aires, BdeF, 2017, cap III.

EIDEM, Matías E. *Afectación de la vida privada en la vía pública, Vigilancia con cámaras de seguridad y restricción de derechos fundamentales,* Buenos Aires, Ad Hoc, 2015.

MAIER Julio, B. *Derecho Procesal Penal* Tomo I, 2.a ed., 3.a reimpresión, Buenos Aires, Editores del Puerto s.r.l., 2004

PÉREZ BARBERÁ, Gabriel, "Nuevas tecnologías y libertad probatoria en el proceso penal" en *Nueva Doctrina Penal,* vol. I, 2009, pp. 271-280.

PORTILLO Víctor Hugo, "Aseguramiento vs. retención de datos de tráfico de las comunicaciones electrónicas" en FERRER (comp) *Estudios de Cibercrimen,* Buenos Aires, Olejnik, 2021, pp 119-136.

PORTILLO, Víctor Hugo/ MATTEO Juan Manuel, "Autoincriminación y nuevas tecnologías" en *Sistema penal e informática,* vol. II, 2021, pp 178-189.

SALT, Marcos, *Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ad Hoc, 2017.

VÉLEZ MARICONDE, *Derecho Procesal Penal*, Tomo III, Parte General, Actos procesales*,* Buenos Aires, Editores del Puerto, 2011

Ley Orgánica 13/2015, del 5 de octubre, de 2015 modificación de la Ley de Enjuiciamiento Criminal, publicada en el Boletín Oficial del Estado BOE, 239, EL 6 de octubre del año 2015

Convenio sobre la Ciberdelincuencia, Budapest 23.XI.2001