revista pensamiento penal

Vulneración de las Garantías Constitucionales en la Investigación en entornos digitales

Registro y Análisis de la Evidencia Digital en la investigación penal – Doctrina del Plain View. Con especial referencia a los Nuevos Derechos digitales en España: Nuevos Derechos Constitucionales de Nueva Generación. Derecho a la Protección del Entorno Digital. Garantías constitucionales en el proceso penal. Datos Públicos. Datos de abonado, de tráfico y de contenido. Fallo Halabi. Expectativa Razonable De Privacidad

María Florencia Suarez

"Sólo el logro de un bien supremo para el todo puede dar derecho al Estado a exigir el sacrificio de un bien menor del individuo. Mientras la preponderancia no sea evidente, la libertad natural debe prevalecer" [1]

Todo el andamiaje relativo a las garantías constitucionales y que tienen relación directa con la temática tratada en la presente, se resume en los artículos 18, 19 y 43 de nuestra Constitución Nacional.

[1] "Nur die Erreichung eines uberwiegenden Guts fur das Ganze kann den Staat berechtigen, die Aufopferung eines minderen Guts von dem einzelnen zu fordern. Solange das Ubergewicht nicht evident ist, muB es bei der narurlichen Freiheit bleiben"]. GOTTLIEB SVAREZ, Carl, Vorträge über Recht und Staat. Cologne: Westdeutscher Verlag, 1960, p. 39

Derecho al honor, a la privacidad, a la intimidad, al secreto de las comunicaciones, derecho a la propiedad, derechos que pueden verse afectados por las investigaciones penales en el entorno digital.

Asimismo, resulta importante tener presente el artículo 30 de la Convención Americana de Derechos Humanos que prevé: "Alcance de las Restricciones: 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.

Este artículo es de perfecta aplicación a esta temática. Es decir, la intromisión del Estado arbitraria e irrazonable, en las investigaciones de delitos en la esfera del individuo.

1.- Derecho a la Protección del Entorno Virtual:

Se habla del Nuevo Derecho Constitucional denominado "Derecho a la Protección del Entorno Virtual".

Resulta interesante mencionar la sentencia del Tribunal Superior Sala 2 de lo Penal de España del 10 de marzo de 2016, Sentencia N° 204/2016: "La ponderación judicial de las razones que 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." [2]

2.- Vulneración del Derecho a la Intimidad y Privacidad en la Investigación Entornos Digitales:

Entiendo que actualmente, en la generalidad de los casos penales sometidos a investigación, en un sistema acusatorio, la policía por orden del órgano de investigación -Fiscalía-, llevan a cabo sus investigaciones empleando técnicas de investigación en los entornos digitales y, por lo tanto, se introducen nuevos medios probatorios: lo realizan en toda clase de delitos, no necesariamente, en la investigación de los delitos informáticos propiamente dichos.

Ya sea que se trate de un homicidio, un robo o amenazas, es posible investigar el entorno digital del presunto autor, en la búsqueda de evidencia digital que resultará sin lugar a dudas útil para la resolución de la causa.

Es más, entiendo que, a corto plazo, la evidencia en cualquier causa penal, ya no va a ser física, sino solo evidencia digital.

Ahora bien, la pregunta es: ¿cómo afecta esta actividad desplegada por el Estado en los derechos y garantías de los y las ciudadanas?

Fundamental es tener presente la diferencia sustancial entre la evidencia física y la evidencia digital, diferencia que repercute directamente tanto, en el modo de ejecución de las medidas de investigación, y en las garantías constitucionales de los y las ciudadanas

¿Qué ocurre cuando se ejecuta una orden de allanamiento y posterior secuestro de los equipos informáticos o celulares: ¿dónde buscar la evidencia? Ya que a diferencia de lo que ocurre con los bienes tangibles, por ejemplo, un arma de fuego o estupefacientes, la evidencia digital no es la computadora o el celular, sino que son los datos almacenados.

[2] Sentencia del Tribunal Superior Sala 2 de lo Penal de España del 10 de marzo de 2016, N° 204/2016, en http://www.poderjudicial.es/search/index.jsp

Por lo tanto, las autoridades no saben qué buscar de antemano, y la afectación a la privacidad e intimidad es de tal magnitud, que resultará conveniente legislar sobre la materia.

Dice Orel Kerr, "En los casos tradicionales, los investigadores simplemente enumeran la ubicación de la evidencia física como el lugar donde se realizará la orden. Sin embargo, esto es solo la ubicación física, no del lugar de la evidencia electrónica a buscar. En tal caso, ¿cómo puede la policía satisfacer el requisito de la Cuarta Enmienda de que la orden especifique el lugar para buscar? ¿Debería indicar la orden de allanamiento, el lugar a buscar? [3]

Se debe tener presente que la computadora o el celular, es solo un dispositivo de almacenamiento, no es evidencia. La evidencia digital son los datos almacenados dentro del dispositivo.

De esta apreciación, surge inconvenientes a la hora de aplicar por analogía las mismas reglas a la evidencia física y digital. Y ello repercute en la vulneración de las garantías constitucionales de los y las ciudadanas.

Además, se debe tener presente que la lógica es distinta, según se trata de evidencia física o digital: "*El proceso de autorización es simplemente uno. Las tecnologías informáticas bifurcan el proceso de autorización de su proceso tradicional de un paso a un proceso de dos pasos, creando una necesidad de normas legales para regular el segundo paso*." [4]

Sobre esto, conviene tener presente que las órdenes de secuestro y análisis de evidencia digital, se desarrollan en dos fases: la fase 1, es la del registro físico y por lo tanto, se solicita al juez el allanamiento del domicilio (del lugar físico), para luego llevar a cabo el análisis del dato informático. Análisis que puede ser llevado a cabo "in situ", es decir, en el lugar, o bien, en el laboratorio.

En **Estados Unidos vs. Hill**[5], se trataba de una causa de explotación sexual infantil. Se solicita una orden de allanamiento y le secuestran a Hill, todos los dispositivos.

[3] OREN, Kerr, SEARCH WARRANTS IN DIGITAL ERA, M IS SIS SIP PI LAW J OURNAL, en https://olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf

[4] Op Cit, OREN, Kerr, SEARCH WARRANTS IN DIGITAL ERA, M IS SIS SIP PI LAW J OURNAL, en https://olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf

[5] Estados Unidos vs. Hill, en https://caselaw.findlaw.com/us-9th-circuit/1256638.html

Cuando se realiza el análisis de los dispositivos, solo se encontró evidencia del delito investigado en uno de ellos.

Claramente la intromisión en la privacidad e intimidad, no solo del sospechoso sino de terceras personas fue realmente grave. Tengamos en cuenta que en los dispositivos había información no solo del sospechoso, sino también, de terceras personas.

Y no todos los dispositivos tenían evidencia del delito investigado, solo uno de ellos. Lesionando también el derecho de propiedad de Hill. Ya que, al secuestrarse todos los dispositivos, se vio impedido de utilizarlos por largo tiempo, para su destino.

Por otra parte, también resulta importante destacar el tema de los puntos de pericia o de análisis de la evidencia digital, una vez secuestrado el equipo (Fase 2). Aquí generalmente, se emplean programas, los que, a través de palabras claves o patrones de búsqueda, buscan valga la redundancia, datos que se relacionen con el delito que se está investigando. Es decir, no se busca en cada uno de los archivos que tiene ese equipo, sino que se recurre a estos programas de búsqueda automatizada.

En muchas causas ocurre que los puntos de análisis son amplios. Por ejemplo, es posible destacar el caso **Silk Road**[6]: la ruta de la seda en su traducción al español. Era una web oculta a través de la cual se llevaban a cabo distintas actividades ilícitas, donde se utilizaba el sistema Tor, mediante el cual se facilitaba el anonimato.

La web era empleada por narcotraficantes de todo el mundo para vender sus productos y ofrecer servicios ilícitos, como la venta de números de tarjetas de crédito y licencias para conducir falsas o contenido audiovisual pirata.

El fundador de Silk Road - Ross Ulbricht-, fue condenado a prisión perpetua. Durante el proceso penal, Ulbricht planteó que se violó la cuarta enmienda, ya que la orden de registro debía especificar los elementos a secuestrar. Cuando se peritaron todos los elementos personales, la defensa de Ulbricht, planteó que ello no ocurrió, debido a que la orden era muy amplia.

La Corte de Apelaciones, finalmente manifestó que en la mayoría de los casos es imposible saber previamente los términos o frases para realizar la búsqueda. No se

[6] Caso Silk Road, en https://freeross.org/

puede saber cómo el imputado almacenó la información. Los archivos o documentos pueden presentar nombres distintos, pueden estar encriptados, o a través de un código insertado por el propio sospechoso, es posible evitar que se realice una búsqueda a través de patrones o palabras claves.

De esta manera, el planteo de la defensa del imputado, fue que tendrían que haberse empleado patrones de búsqueda "ex ante". Con la finalidad de reducir al máximo posible la vulneración de la intimidad y la privacidad.

Por otra parte, resulta interesante destacar la Resolución N° 2013-2718, de fecha 15 de noviembre de 2013, del Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica: "Debe tenerse presente que vulnerar la intimidad de un sujeto, cuando mediante una orden de allanamiento ingresamos a su domicilio, es similar a ingresar a su información digitalizada, ya sea porque se secuestró un disco duro, una computadora o un teléfono celular. Acción que como tal se puede desplegar mediante acceso remoto. Pero sin importar la técnica utilizada, esa actuación debe revestirse con similares requisitos procesales y garantías que impidan injerencias arbitrarias en el ámbito de la intimidad. Igualmente, a cuando se accede a un domicilio mediante autorización y presencia judicial, a buscar rastros de la comisión de un hecho delictivo concreto, donde el titular de esos bienes figura como sospechoso. En ese sentido, se ha pronunciado la jurisprudencia costarricense disponiendo que la orden de allanamiento de morada dictada por un juez penal no incluya la potestad de invadir distintos ámbitos de intimidad, como el contenido en documentos almacenados en medios electrónicos (llaves, maya, discos duros, teléfonos celulares, acceso a la nube, etc.). Mediante tal resolución, se aclaró a las partes que, durante la diligencia de registro, por parte del fiscal, se requiere la presencia del juez penal, para seleccionar así la información relevante según la investigación. En esa ocasión se estableció que el acceso a dichos dispositivos, "… no es equiparable a la figura del registro que se prevé en la orden de allanamiento, pues el mismo alude al registro de la vivienda … y, en todo caso, si se aceptara que comprende el registro de los aparatos de cómputo o de almacenamiento de datos, con mayor razón debe practicarlo directa y personalmente el juez, aunque no lo haga en el mismo lugar y momento, sino en uno diferente, pues tal actuación no puede ser delegada, sino excepcionalísimamente (…), el espectro de protección de la intimidad para el domicilio es más reducido, en la actualidad, que ese otro, que puede tener importante cantidad de información (fotos, videos, conversaciones grabadas, etc.). La flexibilización de garantías, propia del Derecho Penal Moderno, ha llevado a los operadores jurídicos a desconocer la literalidad de las normas, y el artículo 1 de

la ley Nº 742530 es diáfano en cuanto establece la necesaria la presencia de juez. Hasta tanto no se reformule norma, la obligación existirá". [7]

Y agrega la resolución comentada …. "Hoy es una realidad que mediante los dispositivos electrónicos se almacena la mayor parte de informaciones privadas y susceptibles de privacidad, por lo que la noción de documentos privados debe ensancharse. Así se lo ilustra el caso en mención: "En el presente asunto, no cabe duda de que las tarjetas SIM que se logran extraer de los celulares que se le decomisaron a los imputados constituyen una forma o medio de registrar información de carácter privado, pues por dicho medio –las tarjetas SIM– no solo existe la posibilidad de almacenar los datos relacionados con el servicio telefónico (datos del teléfono como lo sería el número), sino también otros datos o información de naturaleza privada que pertenece exclusivamente al usuario o dueño del teléfono". Es por ello que para su acceso y registro deben respetarse las normas procesales, so pena de que la información obtenida y las pericias que de ella deriven decanten en elementos probatorios inútiles para el proceso por violentar el derecho de la constitución y los derechos humanos. [8]

Veamos como ejemplo de la situación actual y que también guarda relación con la Doctrina de la Plain View que más adelante mencionaré, una sentencia del Décimo Circuito de Estados Unidos: ***Estados Unidos v. Carey***, 172 F.3d 1268, 1273-75 (10º Cir. 1999).

Este fallo estableció que "un agente extralimitó el margen de una orden para buscar pruebas de venta de drogas cuando "abandonó dicha búsqueda" y en lugar de ello se dedicó a buscar pornografía infantil durante cinco horas. Asimismo, dicho tribunal advirtió en un caso posterior de que "dado que un ordenador puede almacenar tanta información relativa a muchos ámbitos diferentes de la vida de una persona, existe un riesgo mayor de que se entremezclen documentos, lo que conlleva una invasión de la privacidad cuando la policía lleva a cabo una búsqueda de pruebas en un ordenador". Estados Unidos v. Walser, 275 F.3d 981, 986 (10º Cir. 2001). [9]

[7] Op. Cit., Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica. Resolución Nª 2013-2718, de 15 de noviembre de 2013.

[8] Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica. Resolución Nª 2013-2718, de 15 de noviembre de 2013.

[9] Manual de Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigación criminal Sección de Delitos Informáticos y Propiedad Intelectual División de delitos Ministerio de Justicia de Estados Unidos, Julio de 2002.

3.- <u>Datos Públicos</u>:

Existen datos personales que podrán ser utilizados en las investigaciones penales, y donde no se afecte garantía constitucional alguna, ya que son de acceso público, y consecuentemente, no se requerirá orden judicial.

Se trata de aquellos datos de acceso público: por ejemplo, recurrir a los datos públicos en los perfiles de las redes sociales: Facebook.

Aquí encontramos numerosos fallos judiciales que han declarado válida las pruebas incorporadas al proceso penal: ejemplo: el reconocimiento del imputado por su foto de Facebook.

"Confirmación del procesamiento de quien fue reconocido en rueda de reconocimiento, pese al intento de anular el mismo por haber visualizado las víctimas previamente en Facebook imágenes del procesado". Tribunal: Cámara de Apelaciones en lo Penal de Santa Fe, Sala/Juzgado: III, Fecha: 21-jun-2012, Cita: MJ-JU-M-74995-AR | MJJ74995 | MJJ74995.

Este reconocimiento puede ser realizado tanto por el ciudadano (la victima) como por las autoridades policiales al momento de llevar a cabo los métodos de investigación en la persecución de los delitos.

La Cámara del Crimen confirmó un reconocimiento fotográfico a través de Facebook. Fue en el caso de un hombre que fue agredido por el conductor de una moto, luego buscó sus datos y encontró su perfil en la red social. Ello fue el paso previo a buscar el perfil del agresor en Facebook, lo reconoció y se lo manifestó al fiscal que instruyó el caso. El representante del Ministerio Público le recibió nuevo testimonio, ingresó a la red social y obtuvo imágenes del imputado. (Cámara Nacional De Apelaciones En Lo Criminal Y Correccional - Sala 6 de Buenos Aires (4), CCC 520062850/2012/1/CA2.)

De esta manera, en estos casos, el acceso y recolección y posterior ingreso de la evidencia útil al proceso penal, no es invalida, ya que los datos son de acceso público. Es decir, cualquiera puede tener acceso a dicha información, en este caso en particular, el perfil público de Facebook del imputado.

4.- <u>Datos de abonado, de tráfico y de contenido – Fallo Halabi</u>:

En toda comunicación electrónica, se generan datos.

Datos que pueden ser clasificados en tres categorías, y que la Corte Suprema de Justicia en el Fallo Halabi, ha resaltado, cuando hace referencia a los datos de tráfico y de contenido, fallo que se analizará más adelante.

Las categorías de datos informáticos son las siguientes: datos de abonado, datos de tráfico y de contenido.

Es necesario tener presente estas categorías de datos, a los fines de poder evaluar si en el marco de una investigación penal, la obtención de tales datos, puede vulnerar las garantías constitucionales y en su caso, en qué medida se dará esa afectación.

Ya que teniendo presente el fallo Halabi, los datos de tráfico se asimilan a los de contenido, en orden a los requerimientos para acceder a los mismos, es decir, la orden judicial.

Si bien, ello no siempre ocurre así. En muchas jurisdicciones de nuestro país, es el Fiscal – en un sistema acusatorio- quien, con su sola firma, solicita los datos de tráfico. Contraviniendo claramente lo dicho por la Corte en el fallo Halabi.

A continuación, se brindarán definiciones de cada una de las categorías aludidas de datos:

4.1.- **Datos de Abonado**:

Son aquellos datos necesarios para identificar al usuario de un servicio de internet o servicio de comunicación.

Ejemplos de datos de abonado, son los datos de la tarjeta de crédito asociada al servicio, nombre y apellido del usuario, cuenta de correo electrónico asociada al servicio, domicilio registrado en el servicio, números de teléfono asociados al servicio, fecha y hora de creación de la cuenta, información de sesiones iniciadas, formar de pago, entre otros datos.

El 23 de noviembre de 2017, el poder legislativo aprobó el proyecto de ley de adhesión de Argentina al Convenio de Budapest, un convenio internacional sobre ciberdelito. Mediante la Ley 27.411, se aprueba la Convención de Budapest sobre Ciberdelito, publicada en el Boletín Oficial en fecha 15.12.2017.

Se trata del Convenio sobre Cibercriminalidad, conocido como Convenio de Budapest, y resulta ser el único convenio en el mundo en materia de cooperación internacional en la investigación de los delitos.

En dicho convenio es posible extraer diversos conceptos de "datos".

En orden a los datos de abonado, el Convenio de Budapest, en su Art. 18 cuando regula la orden de presentación dice expresamente: **3.** 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.

Esta clase de datos: datos identificatorios o datos de abonado conforme al Convenio de Budapest, pueden ser obtenidos sin orden judicial.

4.2.- <u>Datos de tráfico</u>:

Los datos de tráfico son cualquier dato que esté relacionado a la conducción de una comunicación a través de internet.

En este sentido, ejemplos de esta clase de datos son: la geolocalización, la duración de una llamada, las llamadas entrantes y salientes, la IP (es un número que identifica la interfaz de conexión a red de un dispositivo electrónico).

Como mencionara anteriormente, conforme el fallo Halabi, estos datos pueden ser recabados con autorización judicial, ya que conforme lo manifestó la Corte Suprema de Justicia en ese fallo: "***los datos de tráfico "anudan a los contenidos***".

Un ejemplo claro de esta afirmación sería el siguiente: ingresar a una página web es una comunicación electrónica. Es un dato de tráfico, pero a través de este dato, puedo también conocer el conocer el contenido de la página web. Y, por lo tanto, conocer el dato de contenido. Por ello, es necesario orden judicial cuando se desea obtener los datos de tráfico.

Por su parte, el Convenio de Budapest también brinda una definición de dato de tráfico y dice: por «***datos sobre el tráfico***» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Los datos de tráfico son asimismo denominados como datos asociados o datos transaccionales o metadatos de la comunicación.

4.3.- Datos de contenido:

Por último, los datos de contenido, son el mensaje mismo, y e independientemente del modo de trasmitir ese mensaje, ya que puede ser por correo, por Whatsapp, etc. Es el contenido mismo de la comunicación. En una comunicación por correo tradicional, el contenido es lo que lee el receptor del mensaje. Lo propio ocurre con una comunicación electrónica.

5.- Fallo Halabi:

El abogado Ernesto Halabi [10]interpuso acción de amparo en virtud de considerar que las disposiciones de la ley 25.873 y de su decreto reglamentario 1563/04 vulneran los derechos establecidos en los artículos 18 y 19 de la Carta Constitucional en la medida en que autorizan la intervención de las comunicaciones telefónicas y por Internet sin determinar "en qué casos y con qué justificativos" esa intromisión puede llevarse a cabo. La referida intervención importa una violación de sus derechos a la privacidad y a la intimidad, y además pone en serio riesgo el "secreto profesional"

[10] Fallo Halabi, Ernesto c/ P.E.N. - ley 25.783 - dto. 1563/04 s/ amparo ley 16.986, Sentencia

24 de febrero de 2009, Id SAIJ: FA09000006.

que como letrado se ve obligado a guardar y garantizar (arts. 6° inc. f, 7°, inc. c y 21, inc. j, de la ley 23.187).

La corte se pronunció en relación con las comunicaciones: "las comunicaciones a las que se refiere la ley 25.873 y todo lo que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional. El derecho a la intimidad y la garantía consecuente contra su lesión actúa contra toda "injerencia" o "intromisión" "arbitraria" o "abusiva" en la "vida privada" de los afectados (conf. art. 12 de la Declaración Universal de Derechos Humanos y art. 11, inc. 2°, de la Convención Americana sobre Derechos Humanos Tratados, ambos, con jerarquía constitucional en los términos del art. 75, inc. 22, de la Constitución Nacional y art. 1071 bis del Código Civil)."

Acerca de estas situaciones este Tribunal ha subrayado que sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos: 306:1892; 316:703, entre otros). Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (confr. art. 236, segunda parte, del Código Procesal Penal de la Nación, según el texto establecido por la ley 25.760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el artículo 18 de la ley 19.798 que establece que "la correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente".

"… es evidente que lo que las normas cuestionadas han - ley 25. dto. 1563/04 s/ amparo ley 16.986. -establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los ***datos de navegación anudan a los contenidos***. Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales. En suma, como atinadamente

ha sido juzgado en autos, resulta inadmisible que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la Administración quede en manos de la más libre discreción de estos últimos, afirmación que adquiere primordial relevancia si se advierte que desde 1992 es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del poder político, la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos. Ello es así por cuanto, en el marco de la transferencia de la prestación del servicio de telecomunicaciones de la ex Empresa Nacional de Telecomunicaciones a licenciatarias privadas, el decreto 1801/1992 dispuso que la Dirección de Observaciones Judiciales de aquella empresa estatal pasara a depender de la SIDE, a los fines de cumplir con dichos requerimientos de los jueces."

6.- Doctrina del Hallazgo A Simple Vista o Plain View Doctrine – Aplicación en el marco de Investigaciones en el Entorno Digital:

Harris vs. USA de 1947[11]

El caso se da en el marco de una investigación sobre violación de la Ley de Fraude Postal y Ley Nacional de Propiedad robada. Cinco agentes federales arrestaron a un sospechoso, en la sala de estar de su departamento. Y sin orden de allanamiento, registraron la vivienda, durante cinco horas. Los agentes buscaban dos cheques cancelados, y cualquier otra evidencia relacionada con la supuesta comisión del delito.

En el cajón de la cómoda de su dormitorio, debajo de ropa del sospechoso, los agentes encontraron un sobre sellado con la inscripción "documentos personales".

El sobre fue abierto, y encontraron varias tarjetas de reclutamiento de propiedad de los Estados Unidos. Lo cual constituía un delito federal. Posteriormente fue condenado por dicho delito.

[11] Harris vs. USA, en https://supreme.justia.com/cases/federal/us/390/234/

Se consideró que la evidencia no se obtuvo lesionando la Cuarta Enmienda, que prevé garantías contra los registros e incautaciones ilegales.

Tampoco, se lesionó la garantía del imputado que prohíbe la autoincriminación.

En este sentido, un registro no se invalida por el hecho de que se haya extendido a otras partes de la habitación en la que se encontraba demorado el sospechoso.

Asimismo, la Corte Americana concluyó que, si existió autorización para ingresar al departamento, la Cuarta Enmienda no prohíbe la incautación por parte de los agentes federales de la evidencia de otro delito. Aun cuando los agentes no tengan conocimiento de la existencia de dicha evidencia, cuando comenzaron el registro.

Por lo tanto, si los agentes que están autorizados por la orden de allanamiento, encuentran sorpresivamente y a simple vista, es decir, por los sentidos, evidencia relacionada con otro delito hasta ese momento desconocido, y por dicho motivo, no hayan sido consignadas en la respectiva orden de allanamiento, pueden secuestrarla informándolo al juez.

Este es el origen de la Doctrina de la Plain View o hallazgo a simple vista o por los sentidos.

Luego vendrá el Fallo ***Horton vs. California***.

Aquí, el oficial de policía, inició una búsqueda autorizada por orden judicial, en la vivienda de un sospechoso por el delito de robo.

La orden de allanamiento solamente mencionaba la búsqueda del producto del robo, pero no de armas. En Horton, la Corte estableció, que los funcionarios a quienes se encomendó el cumplimiento del allanamiento no están impedidos de secuestrar elementos demostrativos de la comisión de un delito distinto de aquel por el cual se libró la orden de ingreso, si la existencia de aquellos elementos fue advertida por accidente o "a franca o simple vista". Si puede procederse así, válidamente, con relación a elementos de un hecho distinto del investigado en la causa que motivó la orden de allanamiento, no cabe invalidar la actuación de los funcionarios intervinientes en este caso, en el cual los elementos secuestrados se vinculan estrechamente con los sucesos investigados.

Citando ***Coolidge vs. New Hampshire***, la Corte Americana afirmó la doctrina básica de que "el oficial de policía tenía una justificación previa para una intrusión en el curso de la cual se encontró inadvertidamente con una pieza de prueba que

incriminaba al acusado. Sin embargo, dispuso dos limitaciones: "que la simple vista por sí sola nunca es suficiente para justificar la incautación de pruebas sin orden judicial" y "que el descubrimiento de pruebas a simple vista debe ser ***inadvertido***.

Como manifiestan en su obra, Chiara Díaz – Obligado: "Puede ocurrir que en el estricto cumplimiento de la orden de allanamiento, la policía encuentre objetos que evidencien la comisión de un delito distinto al que motivó la orden. Por ejemplo, puede ocurrir que el juez emita la orden de allanamiento buscando facturas apócrifas vinculadas con el delito de asociación ilícita tributaria (art. 15c, Ley 24769) y que la DGI y la policía se topen con estupefacientes o con un cadáver. En estos casos, art. 224, parr. 5, CPPN autoriza al personal policial a secuestrar estos elementos con los cuales se topa a simple vista. Esta solución se conoce como doctrina del Plain View y fue elaborada por la Corte Suprema de Justicia de los Estados Unidos en los casos "Harris vs. United States", Coodlige vs. New Hampshire" y "Horton vs. California". [12]

Un problema distinto a la aplicación de la doctrina del Plain View se presenta cuando la policía utiliza la orden de allanamiento de modo discrecional, por ejemplo, entra y sale de la vivienda varias veces invocando la misma orden, o prolonga la duración de la diligencia con el mismo fundamento. [13]

En Argentina, es posible mencionar el precedente de la Corte Suprema "***D' acosta, Miguel Ángel***" - CSJN - 09/01/1987.

El 14 de febrero de 1983, procedió a la detención de Miguel A. D'Acosta, quien se encontraba prófugo por haberse evadido de la Alcaidía de Neuquén el día 28 de noviembre de 1982, donde se encontraba detenido a disposición del juez en lo penal de Cutral Co, Provincia del Neuquén, y que también era buscado por haberse resistido mediante disparos de armas de fuego a su detención, unos días antes de que ésta en definitiva se efectivizara.

En el lugar de la detención, los funcionarios policiales labraron un acta en la que se expresa que se constituyeron en el domicilio indicado "donde se presume se encontraría refugiado el malviviente Miguel A. D'Acosta", con un testigo llamado al efecto, y que inmediatamente procedieron a entrar a la vivienda "ya que la puerta principal se encuentra abierta". Con posterioridad a la aprehensión del prófugo y de

[12] CHIARA DIAZ – OBLIGADO, Garantías, Medidas Cautelares e Impugnaciones en el Proceso Penal, Pág. 87/88.

[13] Op. Cit. CHIARA DIAZ – OBLIGADO, Garantías, Medidas Cautelares e Impugnaciones en el Proceso Penal

otras dos personas, se secuestró un revólver, calibre 38 largo, con la carga completa, sin marca visible y con un número en la base de la culata 6675, y una funda de paño con la inscripción "relojes Pomar", con cinco balas del mismo calibre.

El mismo día, a las dieciséis y cuarenta, la comisión policial se volvió a constituir en el domicilio indicado con la detenida María T. Botegui, a raíz de manifestaciones que la nombrada habría efectuado ante los preventores sobre la existencia de más armas, conforme su declaración testimonial.

Allí se labró una nueva acta en la que consta que dentro de un taparrollos del dormitorio principal se encontró una cartera color suela que contenía en su interior un revólver marca Colt, calibre cuarenta y cuatro, con seis proyectiles intactos, que registraba en su cañonera un número "apenas legible" 41905, otro revólver cromado calibre 38 largo, sin proyectiles, con un sello impreso con la inscripción "detective" y un número en la base de la culata 96464, un trozo de telgopor que contenía seis balas intactas calibre treinta y ocho corto, y una bala nueve milímetros.

Consecuentemente, se imputó a Miguel A. D'Acosta, y finalmente, el juez federal de Morón, Provincia de Buenos Aires, lo condenó a la pena de 4 años de prisión.

La defensa planteó que la pesquisa domiciliaria realizada por las autoridades de prevención, a raíz de la cual se secuestró el arma cuya tenencia se imputó al procesado, constituye un acto que vulneró la garantía constitucional de la inviolabilidad del domicilio (art. 18, Constitución Nacional), porque en el caso los funcionarios no contaban con una orden de allanamiento expedida por un juez, como lo exige el art. 188 del Cód. de Proced. en Materia Penal. Concluye el defensor que, establecida la invalidez del registro domiciliario, igual suerte debe correr el secuestro practicado en esa circunstancia, por lo que resulta inhábil para fundar la sentencia en él.

La Corte manifestó *que no se trata en el caso de establecer si durante un allanamiento realizado con fines de aprehender al presunto delincuente la policía judicial se encuentra habilitada para secuestrar elementos que puedan constituir prueba de la comisión de algún delito, sino de determinar si puede afirmarse que, concluida esa diligencia, el domicilio ha perdido la protección constitucional como consecuencia de aquélla, y ha quedado sujeto a cualquier nueva pesquisa que pudieran realizar los agentes de prevención, sin necesidad de requerir una orden judicial.*

Que la orden de allanamiento que regula la ley procesal, no constituye un acto por el cual el juez delega su "imperium" en un funcionario de policía u otra autoridad, susceptible de ser utilizado

discrecionalmente por ésta, sino que por el contrario, es un mandato singular que se agota con el cumplimiento de la orden, y que no habilita a nuevas entradas.

En efecto, la protección constitucional del domicilio no se puede anular absolutamente, porque esto le estaría vedado aun a los jueces, y la orden de allanamiento sólo tiene por efecto franquear este domicilio al único fin de realizar una diligencia concreta.

Por cierto, mientras dura la diligencia se encuentra enervado el derecho de exclusión del habitante de la morada, de modo que carecerían de eficacia las objeciones que pretendiera oponer a cualquier acto que constituyera una ampliación del objeto de la pesquisa, porque su intimidad ha sido en concreto desguarnecida por mandato judicial. Pero una vez que la pesquisa ha concluido, recupera su derecho de oponerse a la entrada de un tercero ajeno a la morada, aun en el caso de encontrarse en la imposibilidad material de repeler la entrada. [14]

Ahora se debe hacer un paralelismo con la evidencia digital, y en dicha tarea, resulta interesante destacar, que, en el ámbito de la ciudad Autónoma de Buenos Aires, se encuentra el fallo emitido en el Expte N° 8235-00-00-15 - "N. N." - CÁMARA DE APELACIONES EN LO PENAL, CONTRAVENCIONAL Y DE FALTAS DE LA CIUDAD DE BUENOS AIRES - SALA III - 29/04/2016: En el caso, "*corresponde confirmar la resolución de grado que rechazó la nulidad parcial del secuestro practicado en autos. En efecto, la Magistrada de grado dispuso que si durante el desarrollo del allanamiento se verificare la posible comisión de un delito de acción pública que no se encuentre comprendido ni se vincule con el objeto de esta investigación, como la posible comisión de las conductas previstas en el artículo 128 del Código Penal, el personal interviniente deberá entablar inmediata consulta con el Juez Penal y/o con el representante del Ministerio Público Fiscal que por turno y en razón de la materia corresponda.*"

"Del acta policial surge que, ante el análisis de uno de los pendrive encontrados en el cual surgió una vista fotográfica donde se observa a un masculino con una femenina practicándole sexo oral -de la cual se puede presumir que se trataría de una menor de edad- en una cama donde las sábanas y el acolchado son coincidentes con los de la habitación matrimonial del inmueble objeto de la medida. En virtud de ello es que se procede a buscar las prendas de vestir que lleva puesta el femenino en la fotografía y, en dicha búsqueda se encuentra ropa de talles pequeños que presentaban manchas a la altura genital."

"De un informe confeccionado por el Cuerpo de Investigaciones Judiciales, que participó en el allanamiento, se describen con precisión las razones por las cuáles se resolvió inspeccionar la morada a los efectos de determinar la presencia de ciertos elementos probatorios que guardaban relación

[14] Sentencia 9 De Enero De 1987, Corte Suprema De Justicia De La Nación, Id SAIJ: FA87000561.

directa con los archivos que se encontraban examinando en los dispositivos electrónicos tales como: el hallazgo en el dormitorio principal de la vivienda del mismo juego de sábanas y acolchado que se veían en las imágenes fotográficas encontradas, lo que constituirían indicios de que se tratará del mismo domicilio. En razón del hallazgo de estos nuevos elementos probatorios en el inmueble, se procedió a establecer consulta con la Fiscal a cargo de la investigación quien aprobó su secuestro y los remitió al laboratorio químico para que se practiquen los análisis de rigor. Ello así, no se advierten vicios en el procedimiento que permita declarar su invalidez, pues el personal notó -en virtud de que se encontraban abocados a analizar el material obrante en las computadoras y dispositivos informáticos- la similitud entre el escenario de ciertas imágenes pornográficas y la arquitectura y decoración del inmueble en cuestión. (Del voto por ampliación de fundamentos de Dr. Marcelo P. Vázquez). "

Es decir, el personal policial se encontraba analizando los datos en las computadoras. Y a partir de dicho análisis, encontraron imágenes, donde era posible advertir una similitud con el inmueble. Por lo expuesto, la Cámara consideró que no se trataba de un hallazgo casual.

En este caso, se confirmó la resolución de grado que rechazó la nulidad parcial del secuestro practicado en autos. *En efecto, la Defensa se agravió atento que, el Fiscal, en el marco del allanamiento practicado, ordenó el secuestró de ropa de una menor y ropa de cama excediendo la orden de allanamiento. Conforme la doctrina conocida como "plain view doctrine", desarrollada "in extenso" por la Corte Suprema de los EE.UU. (Horton vs. California, 496 U.S. 128), a partir de haberse verificado un ingreso inicial legítimo al domicilio, los funcionarios a quienes se encomendó el cumplimiento del allanamiento no están impedidos de secuestrar elementos demostrativos de la comisión de un delito distinto de aquel por el cual se libró la orden de ingreso, si la existencia de aquellos elementos fue advertida por accidente o "a franca o simple vista". Si puede procederse así, válidamente, con relación a elementos de un hecho distinto del investigado en la causa que motivó la orden de allanamiento, no cabe invalidar la actuación de los funcionarios intervinientes en este caso, en el cual los elementos secuestrados se vinculan estrechamente con los sucesos investigados. (Del voto de Dr. Jorge A. Franza con adhesión de Dra. Silvina Manes).* [15]

7.- <u>DERECHO COMPARADO</u>:

7.1.- <u>ESPAÑA: LEY ÓRGANICA 13/2015, de 5 de octubre de 2015</u>:

[15] Expte N° 8235-00-00-15 - "N. N." - Cámara De Apelaciones En Lo Penal, Contravencional Y De Faltas De La Ciudad De Buenos Aires - SALA III - 29/04/2016, elDial.com - ABD10.

Por su parte, se debe tener presente que, en España, la Ley Orgánica Nº 13/2015, de 5 de octubre de 2015, modificó la Ley de Enjuiciamiento Criminal, con el objetivo de brindar mayor protección a las garantías procesales y reconocer un marco de regulación a las medidas de investigación tecnológica. [16]

Por lo tanto, creó un nuevo artículo 579 bis, el cual prevé específicamente el tema de los descubrimientos casuales.

A título de ejemplo: en su inciso primero, establece que el resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.

Asimismo, prevé que la continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente. Para la cual, el juez debe comprobar la diligencia de la actuación, y evaluará el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento.

Por lo tanto, conforme este artículo, expresamente se prevé que, en el caso de supuestos hallazgos casuales, será el juez el que analizará el contexto dentro del cual se produjo el mismo.

Todo ello a los fines de que la evidencia obtenida sea válida, siempre y cuando sea de conocimiento inmediato al juez competente.

De ahí que, para los efectos de tal prescripción, el material probatorio obtenido casualmente y ajeno al objeto de la investigación sea completamente válido, siempre y cuando tal circunstancia sea puesta inmediatamente en conocimiento del juez competente, y éste, a su vez, resuelva de forma motivada cualquiera de estas dos medidas: o la ampliación de la investigación al ilícito casualmente descubierto, o el inicio de una investigación absolutamente independiente. Ello dependerá, según lo dispone el artículo 17, Nº 1, de la Ley de Enjuiciamiento Criminal, si los nuevos antecedentes constitutivos de delito son o no conexos, vale decir, si existe una relación objetiva y subjetiva entre el hecho punible nuevo y el originalmente investigado. En consecuencia, si los hechos descubiertos tienen una conexión con

[16] Ley Orgánica 13/2015, España, en Boletín Oficial Español, https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725#:~:text=Ley%20Org%C3%A1nica%2013%2F2015%2C%20de,%C2%AB%20BOE%20%C2%BB%20n%C3%BAm.

los que son objeto del procedimiento instructorio, tales hallazgos surtirán efectos tanto de investigación cuanto de prueba; por el contrario, si los hechos ocasionalmente descubiertos no guardan esa conexión, se estimarán como mera "notitia criminis" y deberán ser puestos en conocimiento de la autoridad competente para que se inicie el correspondiente procedimiento. [17]

7.2.- **ESTADOS UNIDOS**:

En el caso Estados Unidos v. Carey, 172 F.3d 1268, 1273 (10° Cir. 1999) un detective de la policía que registraba un disco duro con una orden para buscar pruebas de tráfico de drogas abrió un archivo "jpg" y en lugar de este tipo de pruebas, encontró pornografía infantil.

Llegado a este punto, el detective pasó cinco horas accediendo y descargando varios cientos de archivos "jpg" en un registro cuya finalidad no era la de encontrar pruebas del tráfico de narcóticos para la que se le había autorizado a registrar e inspeccionar de acuerdo con la orden original, sino la de dar con más pornografía infantil.

Cuando el demandado intentó excluir los archivos de pornografía infantil basándose en que se habían confiscado fuera del alcance de la orden, el gobierno adujo que el detective había obrado apropiadamente al confiscar los archivos "jpg" porque el contenido de los archivos de contrabando estaba a simple vista.

El Décimo Circuito rechazó este argumento con respecto a todos los archivos salvo para la primera imagen "jpg" que recuperó el detective.

En el caso Carey, se concluyó que el detective podía confiscar la primera imagen "jpg" que se puso a simple vista mientras estaba realizando el registro con una orden, pero no podía acogerse a la excepción de simple vista para justificar el registro únicamente con el objetivo de buscar más archivos "jpg" con pornografía infantil en los ordenadores del demandado, ya que estas pruebas escapaban al alcance de la orden. [18]

[17] OJEDA, CALFURRAPA Y AKKRASS, Los hallazgos casuales en las diligencias de incautación e intervención de las comunicaciones digitales en Chile. Algunos problemas.

[18] Manual de Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigación criminal Sección de Delitos Informáticos y Propiedad Intelectual División de delitos Ministerio de Justicia de Estados Unidos, Julio de 2002.

Por su parte, en el caso Estados Unidos vs. Walser, del 10° Cir. Año 2001, se concluyó que no hay vulneración a la Cuarta Enmienda, ya que el oficial de policía, quien contaba con una orden judicial para registrar en busca de registros electrónicos de transacciones de drogas, abrió un único archivo informático que contenía pornografía infantil. En consecuencia, el oficial procedió a suspender la búsqueda. E inmediatamente, solicitó al juez una segunda orden para realizar un nuevo registro en busca de pornografía infantil. [19]

Por último, mencionar el caso "***Estados Unidos vs. Henry Franklin Reddick***.

Se trata de un caso, donde empresas privadas dedicadas a la investigación, emplean software para realizar búsquedas automatizadas, y combatir la distribución de pornografía a través de internet.

En este caso se analizó, si el empleo de dicho software por parte de los investigadores, que les permite identificar material sospechoso dentro de cantidades enormes de datos digitales, vulnera o no la Cuarta Enmienda, la cual garantiza a los individuos el derecho a estar seguros en su persona, su domicilio, sus papeles y sus posesiones contra las búsquedas y requisas arbitrarias del estado.

Aquí se empleó el mismo criterio que en el fallo mencionado de España (Tribunal Supremo N°239/2014, del 1 de abril del 2014), y se distinguió entre las búsquedas realizadas por el Estado y los particulares. "Bajo la doctrina de la búsqueda privada, la Cuarta Enmienda no se ve afectada cuando el estado no es el que conduce la búsqueda, sino que recibe y utiliza la información descubierta por una tercera parte privada que es la que conduce la búsqueda. "[20]

El imputado Reddick subió a la nube de Microsoft Sky Drive archivos de imágenes digitales. SkyDrive por su parte, escanea automáticamente los valores hash de los archivos subidos por los usuarios y los compara con los valores de imágenes ya establecidas como pornografía infantil. Cuando el software detecta una coincidencia, genera lo que se llama un "CyberTip" y reenvía el archivo, junto con la información de dirección de IP, al Centro de Niños Perdidos y Explotados, NCMEC.

[19] Estados Unidos vs. Walser, en https://judicialcaselaw.com/courts/iand/cases/2_10-cr-01001-LRR/0751911818

[20] "UNITED STATES of America, Plaintiff-Appellee v. Henry Franklin REDDICK, Defendant-Appellant" - CÁMARA DE APELACIONES - Décimo Circuito - 17/08/2018, 900 F.3d 636 (2018) -

Asimismo, NCMEC reenvió la información al departamento de policía de Corpus Christi, quien asignó a un oficial la tarea de abrir cada archivo y confirmar si cada uno contenía pornografía infantil. El oficial a cargo, solicitó y recibió una orden judicial para realizar un allanamiento en el domicilio de Reddick y requisar su computadora y cualquier material relacionado. Mediante este procedimiento se descubrió más material de explotación y abuso sexual infantil en posesión del imputado.

El imputado presentó una moción para suprimir toda la evidencia de pornografía infantil planteó que la apertura de los archivos asociados con los CyberTips se había realizado sin una orden judicial y por lo tanto era inconstitucional. Y, en consecuencia, solicitó que toda la evidencia de posesión de pornografía encontrada en su hogar debería ser excluida, ya que la revisión inicial del material fue impropia.

Se aplicó la doctrina de la búsqueda privada, y, por lo tanto, se entendió que el oficial no lesionó los derechos tutelados por la Cuarta Enmienda.

Y se resolvió: "Se aplicó lo argumentado en una sentencia anterior sobre un tema de estupefacientes y la corte entendió que cualquier expectativa de privacidad que Reddick tenía en los valores hash de sus archivos, fue frustrada por la búsqueda automática y privada de Microsoft. Cuando las autoridades recibieron los archivos subidos por el imputado, ya se había establecido que había una coincidencia entre sus valores hash y aquellos de imágenes reconocidas como pornografía infantil. Es decir que no hay, por parte de las autoridades policiales, una expansión de la búsqueda inicial hecha por la entidad privada como para entender que el accionar de las autoridades constituye una nueva búsqueda".

8.- **Expectativa Razonable De Privacidad**:

La expectativa razonable de privacidad es un criterio que ha sido empleado para determinar si se han vulnerado garantías constitucionales.

"Los requisitos que debe cumplir la expectativa razonable de privacidad consiste en atender pruebas objetivas y subjetivas de racionalidad. La prueba objetiva requiere que toda persona razonable asuma de manera efectiva la expectativa de privacidad. Por otra parte, la prueba subjetiva requiere observar que efectivamente exista una expectativa de privacidad genuina. Aunque es posible pensar que contamos con una expectativa razonable de privacidad en nuestros dispositivos electrónicos, se han

reconocido límites y por tanto, existen circunstancias especiales que pueden anular dicha expectativa."[21]

Por ejemplo, una persona no tendrá expectativa alguna de privacidad si ha hecho pública la información almacenada en el ordenador.

En el caso Estados Unidos vs. David, los agentes obtuvieron la contraseña del demandado al mirar por encima del hombro de éste y verla en la pantalla cuando la tecleó en un ordenador portátil. El tribunal no halló indicios de infracción de la Cuarta Enmienda en la obtención de la contraseña, ya que el demandado no gozaba de una expectativa razonable de privacidad "en lo que aparecía en la pantalla". [22]

Asimismo, en el caso Katz vs. Estados Unidos, "aquello que una persona haga del dominio público, aunque lo haga desde su casa o despacho, no está sujeto a la protección de la Cuarta Enmienda").; Estados Unidos v. Gorshkov, 2001 WL 1024026, en *2 (W.D. Wash. 23 de mayo de 2001) (en la que se sostiene que el demandado no tenía ninguna expectativa razonable de privacidad en el uso de una red informática privada cuando los agentes secretos miraron por encima de su hombro, al no ser el propietario del ordenador que estaba utilizando y al saber que el administrador del sistema podía vigilar lo que hacía). Asimismo, las personas tampoco pueden tener una expectativa razonable de privacidad en el contenido de un ordenador que hayan robado. Véase Estados Unidos v. Lyons, 992 F.2d 1029, 1031-32 (10º Cir. 1993). [23]

En el caso Carpenter vs. Estados Unidos[24], la Corte Suprema se pronunció sobre la expectativa razonable de privacidad, cuando se trata de la vigilancia del gobierno captando las señales del celular: En el año 2011, la policía arrestó a cuatro hombres sospechosos de robar tiendas de móviles en Detroit. Uno de los hombres confesó que, durante los cuatro meses anteriores, junto con otras personas había robado nueve tiendas diferentes en Michigan y Ohio. El sospechoso identificó a 15

[21] En busca de la privacidad perdida "Carpenter vs. Estados Unidos" Juan Antonio Travieso, Tomo LA LEY 2019-B

[22] Op. Cit, Manual de Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigación criminal Sección de Delitos Informáticos y Propiedad Intelectual División de delitos Ministerio de Justicia de Estados Unidos, Julio de 2002.

[23] Manual de Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigación criminal Sección de Delitos Informáticos y Propiedad Intelectual División de delitos Ministerio de Justicia de Estados Unidos, Julio de 2002.

[24] Carpenter vs. Estados Unidos, Año 2018, en https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

cómplices que habían participado en los atracos y le dio al FBI algunos de sus números de teléfono celular.

El FBI luego revisó sus registros de llamadas para identificar números adicionales. Aquí la Corte manifiesta que "Permitir que el gobierno acceda a los registros de los sitios celulares contraviene esa expectativa. Aunque dichos registros se generan con fines comerciales, esa distinción no niega la idea de Carpenter de la privacidad en su ubicación.

Con base en esa información, los fiscales solicitaron órdenes judiciales en virtud de la Ley de comunicaciones para obtener registros de teléfonos celulares de Timothy Carpenter y otros sospechosos. Esta legislación permite al Gobierno obligar a la divulgación de ciertos registros de telecomunicaciones cuando se demuestre que existen

motivos para creer "que los registros buscados" son relevantes y evidencia para una investigación criminal en curso ". Los magistrados federales emitieron dos pedidos dirigidos a los proveedores de servicios inalámbricos de Carpenter. En total, el gobierno obtuvo 12,898 puntos de ubicación que catalogan los movimientos de Carpenter.

"Mapear la ubicación de un teléfono celular durante el curso de 127 días proporciona un registro completo del paradero del titular. Al igual que con la información del GPS, los datos con marca de tiempo proporcionan una ventana íntima a la vida, revelando no solo sus movimientos particulares, sino a través de ellos sus "asociaciones familiares, políticas, profesionales, religiosas y sexuales". Id., En 415 (opinión de SOTOMAYOR, J.). … Si bien las personas abandonan regularmente sus vehículos, llevar consigo teléfonos móviles compulsivamente todo el tiempo. Un teléfono celular sigue fielmente a su dueño más allá de las vías públicas y hacia residencias privadas, consultorios médicos, sede política …"

En consecuencia, cuando el Gobierno rastrea la ubicación de un teléfono celular logra una vigilancia perfecta, como si hubiera conectado un monitor de tobillo al usuario del teléfono."

Por su parte, en España, se destaca la sentencia del Tribunal Supremo N°239/2014, del 1 de abril del 2014, la cual no admitió las grabaciones de una cámara colocada por el empresario en el despacho del empleado sin contar con su consentimiento ni con autorización judicial. Las cámaras se habían colocado ante las sospechas de que el trabajador, encargado de la contabilidad, estaba distrayendo dinero de la caja, y se

habían colocado en diferentes lugares. Por medio de ellas se descubre que, efectivamente, este trabajador estaba apartando dinero y haciendo manipulaciones en las facturas y es condenado por apropiación indebida. [25]

El acusado interpuso recurso de Casación, ya que consideró que se vulneró su derecho a la intimidad, debido a que se valoró como prueba una grabación obtenida de forma ilegal, al no existir conocimiento del trabajador ni autorización judicial. Señala que la colocación de cámaras en su despacho sin contar con su autorización ni autorización judicial vulnera su derecho a la intimidad, al invadir el terreno personal y privado, así como la presunción de inocencia al basarse la condena en prueba ilícitamente obtenida, por lo que solicita su absolución.

El Tribunal Supremo sostuvo que *no es lo mismo grabar las zonas comunes de trabajo, que el despacho del trabajador, en cuyo interior tiene una expectativa razonable de intimidad que puede verse vulnerada si se instalan cámaras de grabación sin su conocimiento y, por lo tanto, no pudieron tenerse en cuenta las pruebas provenientes de esta cámara como prueba de cargo*".

Es necesario tener presente que esta sentencia cuenta, con un voto particular del Magistrado D. Antonio del Moral García.

En primer lugar, este magistrado manifestó que "Hay que diferenciar zonas y dependencias. No es lo mismo un espacio abierto del centro de trabajo que aquél que puede ser de uso predominantemente individual y personalizado como podría suceder con esa aludida "oficina". De acuerdo con la doctrina del Tribunal Constitucional (en cuya más reciente jurisprudencia se apoya la sentencia mayoritaria - STC 170/2013, de 7 de noviembre) cuando se incide en un derecho fundamental como es la intimidad, se hace indispensable testar para la legitimidad constitucional de la actuación la proporcionalidad (idoneidad, necesidad, proporcionalidad en sentido estricto).

Además, en cuanto a la prueba ilícita, dijo: "Cuando hablamos de prueba ilícita, debe exigirse usando el paralelismo penal una conducta antijurídica y culpable (aunque sea simple negligencia). No es "ilícita" a estos efectos la acción, ni por tanto la prueba, cuando se ha actuado de buena fe, con la convicción de que la conducta se ajustaba al ordenamiento y sin indiligencia, indiferencia o desidia reprobables.

[25] Sentencia Tribunal Supremo N°239/2014, del 1 de abril del 2014, en http://www.poderjudicial.es/search/index.jsp#

Este voto particular, hace referencia a la vulneración de las garantías cuando provienen de un particular, y no del Estado: "… se trata de una ilicitud atribuible no a órganos del Estado, sino a particulares.

No hay duda de la eficacia de los derechos fundamentales entre particulares (drittewirkung), aunque no se puede desconocer que su construcción teórica y su fortificación legal y práctica ha surgido y crecido sobre todo en tensión frente a los poderes estatales.

Por definición algunos derechos fundamentales solo son oponibles al poder estatal (derecho a no confesarse culpable -con algún matiz-, y en general, derecho a un proceso con todas las garantías). Es verdad que el art. 11.1 LOPJ no introduce distinción alguna en este sentido.

La inutilizabilidad de la prueba obtenida con violación de derechos se predica de todos los casos y de todos los procesos, más allá de que el agente infractor sea estatal o un particular. También en el proceso civil …. o en el laboral rige la previsión. Pero, admitido eso, no puede ocultarse que por tradición, por teleología, por ponderación de derechos fundamentales en tensión y por sus finalidades, el juego de esa norma, de máxima intensidad cuando la violación proviene de un agente estatal, consiente más modulaciones en el caso de particulares (son frecuentes en el derecho comparado las regulaciones de esta materia. "

Y agrega: "Un dato clave es que no estamos solo ante un tema laboral. No se trata de un sistema de vídeo grabación establecido con carácter estable y preventivo, lo que exigiría advertir a los afectados. Si es subrepticio un sistema preventivo de control en un lugar individual difícilmente podrá justificarse. Pero estamos ante una cámara instalada de manera puntual con el objetivo de descubrir un delito. Concurren indicios y razones para pensar que de esa forma se iba a poder no solo esclarecer; sino también evitar la continuidad de la actuación delictiva. No se trata solo de sancionar (descubrir el delito cometido), sino de que la víctima quiere abarcar con el atentado en su patrimonio que persiste. No nos movemos en el territorio de la prevención, o del control laboral, sino de defensa del propio patrimonio: recordemos la mención específica que en el art. 20. 4º CP se hace a la legítima defensa de los propios bienes.".

Por su parte, conviene mencionar un caso de Estados Unidos, referente en materia de expectativa razonable de privacidad.

Se trata del caso Estados Unidos vs. Jones, de fecha 23/01/12.

Aquí, el Gobierno obtuvo una orden judicial de búsqueda que le permitía instalar un dispositivo de localización (GPS) en un automóvil registrado a nombre de la esposa del demandado Jones.

La orden judicial autorizó su instalación en el Distrito de Columbia y dentro del plazo de diez (10) días, pero los agentes instalaron el dispositivo el día undécimo y en el Estado de Maryland. Luego, el Gobierno siguió los movimientos del vehículo durante veintiocho (28) días. Posteriormente logró obtener evidencia para acusar a Jones y a otras personas por los delitos de tráfico de estupefacientes y de conspiración. [26]

Vemos que aquí, la orden era limitada en el tiempo, es decir, 10 días. Asimismo, se especificaba el lugar. Todo ello, con la finalidad de reducir al máximo posible la invasión a la privacidad e intimidad.

Sin embargo, los agentes policiales, se extralimitaron.

El tribunal federal de primera instancia descartó los datos del GPS obtenidos mientras el automóvil había estado estacionado en la casa de Jones, pero consideró el resto de los datos admisibles porque Jones no tenía ninguna expectativa razonable de privacidad cuando el vehículo se encontraba en la vía pública. Jones fue condenado.

Finalmente, el Tribunal Federal de Circuito con asiento en el Estado de Columbia revocó la sentencia y consideró que la admisión de las pruebas obtenidas mediante el uso del dispositivo GPS sin orden judicial viola la IV Enmienda a la Constitución de los Estados unidos.

"La instalación del dispositivo GPS en el vehículo, ordenada por el Gobierno, y la utilización de ese recurso para controlar los movimientos del automóvil constituyen un registro en términos de la IV Enmienda."

La IV Enmienda protege el "derecho de las personas a su seguridad física, domicilios, papeles y efectos contra registros y detenciones arbitrarias".

"Esta conclusión se compadece con la jurisprudencia de este Tribunal relativa a la interpretación de la IV Enmienda, la cual hasta la segunda mitad del siglo XX estuvo

[26] Estados Unidos vs. Jones, de fecha 23/01/12, en http://www.casebriefsummary.com/united-states-v-jones/

ligada a la acción de daños y perjuicios del common law. En los casos recientemente resueltos nos apartamos de ese criterio basado exclusivamente en la propiedad y aplicamos el análisis propuesto en el voto concurrente del Justice Harlan en Katz vs. United States (389 U.S. 347 -1967-), conforme al cual la IV Enmienda protege la "expectativa razonable de privacidad" de una persona."

"Estados Unidos vs. Knotts (460 U.S. 276 -1983-) y Estados Unidos vs. Karo (468 U.S. 705 -1984-) -casos posteriores a Katz que rechazan los cuestionamientos de la IV Enmienda a los "localizadores", dispositivos electrónicos de seguimiento que representan otra forma de monitoreo electrónico- no descartan la conclusión de que aquí haya tenido lugar una pesquisa. Tampoco Nueva York v. Clase (475 U.S. 106 -1986-) ni Oliver v. United States (466 U.S. 170 -1984-) brindan sustento la posición del Gobierno. [27]

9.- **Conclusiones**:

Se debe comprender, la dificultad que se plantea, en orden a la diferencia misma entre investigaciones en entornos físicos y en entornos digitales.

Es muy difícil saber previamente dónde buscar la evidencia, ya que un archivo puede ser guardado en la computadora de diversas formas, extensiones y nombres.

Porque entiendo hay una gran diferencia entre, por ejemplo, un allanamiento donde se busca mercadería robada, o estupefacientes, y además en el lugar y a simple vista, se encuentra un arma de fuego.

De lo que ocurre cuando se investiga la computadora del sospechoso y se encuentra en forma "casual" o "a simple vista" material de explotación o abuso sexual de menores. La pregunta es ¿Cómo es posible determinar cuándo se está en presencia de un hallazgo casual, en este contexto?

La investigación en entornos digitales, requiere de reglas claras desde el punto de vista de las garantías constitucionales. Ya que es mucho más intrusivo abrir una computadora y empezar a investigar qué tiene esa computadora.

[27] United States v. Jones - 23-1-12, en https://www.csjn.gov.ar/dbre/Sentencias/usJones.html

La lógica es distinta según se trata de investigaciones en entornos físicos y entornos digitales.

Y entiendo que esa lógica requiere que se aborde el problema estableciendo reglas claras a los fines de cumplir con el mandato constitucional. Y evitar lesionar el derecho a la intimidad, la privacidad, la propiedad y la garantía que prohíbe la autoincriminación del sospechoso.

Resulta imperioso una regulación de la temática, ya que no es lo mismo que en el marco de un allanamiento, donde se busca un arma de fuego, y luego de su hallazgo, la intromisión termina.

A que, por el contrario, se disponga el allanamiento, registro y secuestro de una computadora, cuando la información almacenada es en gran cantidad, con seguridad hay información sensible que nada tiene que ver con el delito que se está investigando, de propiedad no solo del sospechoso sino de terceras personas.

Por lo tanto, siempre se requerirá autorización judicial, si se encontraren evidencias relacionadas con la presunta comisión de otro delito -distinto al que motivó la orden judicial-.

Además, el fiscal en un sistema acusatorio deberá acreditar fehacientemente, que se ha tratado efectivamente de un hallazgo casual.

¿Cómo se acredita que ha sido un hallazgo casual, cuando se registra una computadora o un teléfono móvil? Ya que se debe tener presente que no hay límites físicos cuando hablamos de evidencia digital.

Por ello, es que la lógica es diversa, y las reglas del juego deben ser diversas, más acorde con la naturaleza de la evidencia digital.

Bibliografía:

1.- Sentencia del Tribunal Superior Sala 2 de lo Penal de España del 10 de marzo de 2016, N° 204/2016.

2.- OREN, Kerr, Search Warrants In Digital Era, MISSISSIP PILAW JOURNAL.

3.- Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica. Resolución N° 2013-2718, de 15 de noviembre de 2013.

4.- Manual de Registro y confiscación de ordenadores y obtención de pruebas electrónicas en investigación criminal Sección de Delitos Informáticos y Propiedad Intelectual División de delitos Ministerio de Justicia de Estados Unidos, Julio de 2002.

5.- CHIARA DIAZ – OBLIGADO, Garantías, Medidas Cautelares e Impugnaciones en el Proceso Penal.

6.- Sentencia 9 De Enero De 1987, Corte Suprema De Justicia De La Nación, Id SAIJ: FA87000561.

7.- Ley Orgánica 13/2015, España, en Boletín Oficial Español.

8.- OJEDA, CALFURRAPA Y AKKRASS, Los hallazgos casuales en las diligencias de incautación e intervención de las comunicaciones digitales en Chile. Algunos problemas.

9.- En busca de la privacidad perdida "Carpenter vs. Estados Unidos" Juan Antonio Travieso, Tomo LA LEY 2019-B.