

Tecnologías de la información y la comunicación e investigación penal

M. Elena Godoy B.

I.- Introducción.

Las tecnologías de la información y la comunicación (TIC's) han significado desde su surgimiento un constante desafío para el sistema penal. Este desafío ha requerido -y, aún requiere- de diversas adecuaciones normativas tanto en el ámbito del derecho penal material como del derecho procesal penal y, en particular, de los mecanismos de cooperación internacional en materia penal¹.

En lo que se refiere al derecho penal material, se produjo en el derecho comparado un proceso de adecuación de las normas penales tradicionales para tipificar estas nuevas modalidades de conductas o formas de comisión de delitos no tradicionales que, por las características de su comisión, no se encontraban alcanzadas por los tipos penales vigentes.

En este sentido, la iniciativa global más relevante fue adoptada en noviembre del 2001, cuando el Consejo de Europa² sancionó el Convenio sobre Ciberdelito³ que constituye el único instrumento internacional que aborda de manera específica la temática del cibercrimen. Instrumento normativo que fue incorporado por la República Argentina mediante la sanción de la Ley N° 27.411⁴.

¹ En el Duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se afirmó que: *“Las dificultades que el elemento transnacional plantea para la investigación del delito cibernético son parecidas a las que entrañan otros delitos transnacionales. Como consecuencia del principio fundamental de la soberanía nacional, según el cual no pueden realizarse investigaciones en territorios extranjeros sin el permiso de las autoridades locales, la cooperación estrecha entre los Estados involucrados es crucial para la investigación de los delitos cibernéticos. Otra dificultad importante se relaciona con el poco tiempo disponible para llevar a cabo las investigaciones de esos delitos. A diferencia de lo que ocurre con las drogas ilícitas, que, según el medio de transporte que se utilice, pueden tardar semanas en llegar a su destino, los correos electrónicos se envían en segundos y, si se tiene acceso a un ancho de banda adecuado, es posible descargar grandes ficheros en algunos minutos... [...]”*. Para mayor información, consultar <http://www.un.org/es/comun/docs/?symbol=A/RES/65/230> Duodécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado del 12 al 19 de abril de 2010, en Salvador, República Federativa de Brasil.

² El Consejo de Europa es una organización internacional creada en 1949 con el fin de promover la cooperación entre los países de Europa y afianzar los valores de la democracia, los derechos humanos y el estado de derecho. En la actualidad abarca a casi todos los países del continente europeo y no debe ser confundido con otros organismos más conocidos como la Unión Europea.

³ Conocido por todos como “Convenio de Budapest” que entró en vigor en 2004. Disponible (en inglés) en: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>

⁴ La Ley N° 27.411 -que aprobó la incorporación del *Convenio sobre Ciberdelito* del Consejo de Europa a nuestro ordenamiento jurídico interno- fue sancionada el 22 de noviembre de 2017 y publicada en el Boletín Oficial el 15 de diciembre de 2017.

Este proceso de modificación de las normas penales sustantivas contrasta significativamente con la escasa repercusión que ha tenido el *mundo virtual* en las normas del derecho procesal penal y de los convenios de cooperación internacional en materia penal, que son imprescindibles para la investigación de estas nuevas formas delictivas.

Pues, para un adecuado tratamiento por parte del sistema de administración de justicia criminal de los delitos informáticos -o de delitos tradicionales para cuya persecución se requiere de evidencia digital- no alcanza sólo con la modificación de las normas penales de fondo.

Antes bien, emerge como indispensable analizar qué herramientas de investigación tecnológica resultan necesarias desarrollar para que los casos penales puedan adquirir los elementos probatorios digitales / evidencias digitales que se transmutarán en pruebas durante la audiencia de juicio. Herramientas que, claramente, presentan características diferentes a las que guiaron las regulaciones de los códigos procesales vigentes, que se encuentran estructurados para la investigación de hechos sucedidos en un espacio físico y no en el espacio virtual⁵.

Resulta evidente de una simple lectura de los códigos procesales que todo el sistema probatorio ha sido diseñado teniendo en cuenta la evidencia física y no la evidencia digital que presenta características absolutamente diferentes y que dificultan la aplicación por analogía de las normas tradicionales⁶.

Sin embargo, en lo que respecta al proceso penal, se advierte una resistencia cultural al cambio o, por lo menos, un menor desarrollo que el alcanzado en la armonización de las normas penales de fondo a las cuestiones novedosas que plantean los sistemas informáticos, ya sea como objeto de delito o como mecanismo de comisión de delitos.

Con todo, en forma previa, la República Argentina, había sancionado la Ley de Delitos Informáticos N° 26.388, el 4 de junio de 2008 y que fue promulgada de hecho el 24 de Junio de 2008.

⁵El lector podrá analizar, a modo de ejemplo, las sustanciales diferencias que tiene la investigación de un delito cometido en un espacio físico (empleado de un banco que sustrae una suma de dinero de la caja de seguridad) con la investigación de un hecho similar pero cometido mediante mecanismos tecnológicos (empleado de un banco que ingresa al sistema informático bancario violando las claves de seguridad y transfiere fondos a la cuenta offshore de su cómplice en el exterior).

⁶ A modo de ejemplo, basta con revisar las normas sobre “registro” y secuestro”, pensadas para evidencias físicas y no para datos electrónicos.

Este escenario propicia la necesidad de analizar, en el ámbito nacional, si las normas procesales tradicionales (códigos procesales penales tanto federal como de las distintas provincias) y las normas que regulan la organización de los distintos sujetos encargados de la persecución penal son las idóneas para hacer frente a los problemas que generan, para el adecuado funcionamiento del sistema de enjuiciamiento penal, las modernas tecnologías de la información y la comunicación (TIC's)⁷.

El objetivo que pretendo abordar en la presente ponencia: es presentar una enunciación de los desafíos principales que presentan las medidas de investigación tecnológica, para proponer un debate que permita analizar en nuestro país su influencia en el proceso penal y sugerir algunas conclusiones generales teniendo como modelo de análisis comparativas las previsiones de la Convención sobre Ciberdelito que aparece hoy como el instrumento internacional que mayor consenso, a nivel global, ha alcanzado.

II.-Breve reseña de antecedentes internacionales relevantes en la temática.

II.1.- La Convención sobre Ciberdelito

La Convención sobre Ciberdelito tiene su origen en la necesidad -de los Estados parte del Consejo de Europa- de establecer de manera prioritaria una política penal común destinada a proteger a la sociedad del crimen en el ciberespacio, mediante la necesidad de armonizar los elementos jurídicos sustantivos que faciliten la detección, la investigación y el enjuiciamiento, tanto en el ámbito nacional como en el internacional, de los ilícitos penales cometidos a través del uso de las TIC's y establecer un sistema rápido y eficaz de cooperación internacional.

En el plano, procesal, la Convención enumera las siguientes herramientas: 1) preservación acelerada de los datos almacenados; 2) preservación acelerada y divulgación parcial de datos de tráfico, 3) ordenes de producción, búsqueda y captura de datos informáticos; 4) recolección en tiempo real de datos de tráfico; 5) la interceptación de datos de contenido; 6) una disposición sobre un tipo específico de acceso transfronterizo a datos

⁷ Para profundizar sobre el impacto de las tecnologías digitales en el proceso penal, véase Kerr, Orin S., *Digital Evidence and the New Criminal Procedure*. 105 Columbia Law Review 279 (2005); GWU Law School Public Law Research Paper N° 108. Disponible en SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101

informáticos almacenados que no requiere asistencia jurídica mutua (con consentimiento mutuo o cuando esté públicamente disponible); y,7) la creación de una red 24/7 para garantizar la rápida asistencia judicial entre los Estados Signatarios de la Convención.

Al mismo tiempo, la Convención requiere la provisión de una protección adecuada de los derechos humanos y las libertades fundamentales, incluidos los derechos que se deriven de conformidad con las obligaciones previstas bajo el Convenio Europeo de Derechos Humanos, el Pacto Internacional sobre Derechos Civiles y Políticos y otros instrumentos internacionales de derechos humanos aplicables, debiéndose incorporar el principio de proporcionalidad⁸.

La Convención ha sido complementada por un Protocolo Adicional⁹ que tipifica la publicación de propaganda racista y xenófoba a través de redes informáticas.

II.2.- Marco normativo y reglas prácticas elaboradas por órganos multilaterales

En el Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se sostuvo que: *“La investigación de la delincuencia informática no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales, que suelen ser volátiles y de vida corta. También se plantean problemas legales en relación con las fronteras y las jurisdicciones.*

La investigación y el enjuiciamiento de delincuentes informáticos ponen de relieve la importancia de la cooperación internacional [...].

⁸ Así el artículo 15.1 denominado **Condiciones y garantías** de la Convención de Ciberdelincuencia establece: *“Cada Parte velará por que el establecimiento, implementación y aplicación de las facultades y procedimientos establecidos en esta Sección estén sujetos a las condiciones y garantías establecidas en virtud del derecho nacional, el cual deberá proporcionar la protección adecuada de los derechos humanos y las libertades fundamentales, incluidos los derechos que se deriven de conformidad con las obligaciones que ha asumido en virtud del Convenio del Consejo de Europa de 1950 para la Protección de los Derechos Humanos y las Libertades Fundamentales, el Convenio Internacional de las Naciones Unidas de 1966 sobre Derechos Civiles y Políticos y otros instrumentos internacionales de derechos humanos aplicables, y los cuales incorporarán el principio de proporcionalidad”.*

⁹ El Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos -en adelante, Protocolo-, fue adoptado por el Consejo de Comité de Europa de Ministros el 7 de noviembre de 2002 y entró en vigor el 1 de marzo de 2006.

El Protocolo exige a los Estados Parte penalizar la difusión de material racista y xenófoba por medio de sistemas informáticos, así como de las amenazas e insultos racistas y motivados por la xenofobia.

La creciente densidad de tecnologías de la información y las comunicaciones también aumenta la frecuencia de la delincuencia informática nacional, obligando a las naciones a establecer legislación nacional. Puede que se requieran leyes nacionales adaptadas a la delincuencia cibernética para responder eficazmente a las peticiones externas de asistencia o para obtener asistencia de otros países. Cuando se elabora legislación, la compatibilidad con las leyes de otras naciones es una meta esencial; la cooperación internacional es necesaria debido a la naturaleza internacional y transfronteriza de la delincuencia informática. Se necesitan mecanismos internacionales formales que respeten los derechos soberanos de los Estados y faciliten la cooperación internacional. Para que la asistencia judicial recíproca funcione con éxito, los delitos sustantivos y los poderes procesales de una jurisdicción deben ser compatibles con los de otras... ”.

En concreto, sobre la cooperación internacional, se sostuvo que: “...La cooperación tempestiva y eficaz entre las autoridades de diferentes países es fundamental también porque en los casos de delitos cibernéticos las pruebas suelen suprimirse automáticamente y al cabo de poco tiempo. Los procedimientos oficiales prolongados pueden obstaculizar seriamente las investigaciones...”¹⁰.

Se tuvo presente también que en los delitos informáticos pueden intervenir grupos delictivos en dos aspectos: el uso de las tecnologías de la información por parte de grupos delictivos tradicionales o la comisión de delitos cibernéticos por grupos delictivos organizados¹¹, que abre la posibilidad de utilizar instrumentos tales como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional¹².

¹⁰Para mayor información, consultar:http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf. Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado del 18 a 25 de abril de 2005, en Bangkok, Tailandia.

¹¹ “[...] los grupos delictivos organizados tradicionales que no tienen antecedentes de actividades delictivas relacionadas con Internet están utilizando la tecnología de la información para coordinar sus actividades y aumentar su eficacia en la comisión de delitos... En estos casos, la tecnología de la información se utiliza para mejorar la eficiencia del grupo delictivo organizado en su campo de actividad tradicional. Ello incluye la utilización de las comunicaciones electrónicas, que le permiten, por ejemplo, hacer uso de la tecnología de cifrado y comunicar en forma anónima... Los informes indican que los grupos delictivos organizados tradicionales están tendiendo a emprender nuevas formas de actividades delictivas en la esfera de los delitos de alta tecnología. Ello incluye la piratería de programas informáticos y otras formas de violación de los derechos de autor. Pero también otras esferas del delito cibernético, como la pornografía infantil y los delitos relacionados con la identidad, están vinculados a menudo con la delincuencia organizada [...]”

¹² La Convención Internacional contra la Delincuencia Organizada Transnacional y sus protocolos complementarios para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños y

En cuanto a la respuesta a esta modalidad delictiva, se destacó que las organizaciones internacionales, las naciones y las fuerzas de seguridad abordaban el fenómeno de diversas formas, que incluyen medios legislativos, de aplicación de la ley y de fomento de la capacidad.

Concretamente respecto a la aplicación de la ley, se dijo que depende en gran medida “[...] de la disponibilidad de instrumentos de investigación tales como programas informáticos forenses (para reunir pruebas, registrar las pulsaciones de teclado y descifrar o recuperar ficheros suprimidos) y programas informáticos o bases de datos de gestión de la investigación (por ejemplo, con valores “hash” para imágenes de pornografía infantil conocidas)”.

Por otra parte, el *Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia*¹³ fue suscripto por los gobiernos de Guatemala, Nicaragua, Portugal, Perú y Uruguay, en la sede de la Conferencia de Ministros de Justicia de los Países Iberoamericanos¹⁴, el 28 de mayo de 2014; en tanto que la *Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia*¹⁵, fue firmada por los gobiernos de Guatemala, Nicaragua, Portugal, Perú y Argentina con la finalidad de lograr un impacto en la legislación nacional de los países miembros de la COMJIB.

Respecto de la importancia de estos instrumentos se indicó: “*El Convenio aporta una amplia definición de Ciberdelincuencia que permite que los instrumentos de cooperación internacional se puedan aplicar para muchos tipos de delitos; y la Recomendación se presenta como un aporte adicional a los Estados para que puedan actualizar y modernizar sus legislaciones penales para combatir de forma efectiva la*

contra el tráfico ilícito de migrantes tierra, mar y aire fue aprobada por Ley N° 25.632, sancionada con fecha 1 de agosto de 2002 y promulgada con fecha el 29 de agosto de 2002.

Disponible

en:

<http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf>

¹³ Disponible en: http://www.comjib.org/sites/default/files/CONVENCION_CIBER.pdf

¹⁴ La Conferencia de Ministros de Justicia de los Países Iberoamericanos en adelante, COMJIB- es una organización internacional que agrupa a los Ministerios de Justicia e instituciones homólogas de los 21 países de la Comunidad Iberoamericana, y que tiene por objeto el estudio y promoción de formas de cooperación jurídica entre los Estados miembros. La Conferencia se reúne de forma plenaria cada dos años y tiene su sede en Madrid, Reino de España.

¹⁵ Disponible en: http://www.comjib.org/sites/default/files/Ciberd_Recomendacion_28052014_0.pdf

cibercriminalidad, y evitar que estos hechos delictivos queden en la impunidad, contribuyendo a la modernización de las legislaciones penales internas de los países”¹⁶.

En el ámbito de las Reuniones Especializadas de Ministerios Públicos del Mercosur (REMPM)¹⁷, la temática del cibercrimen es objeto de análisis específico a raíz de la creación de un sub-grupo de trabajo¹⁸ dentro del Grupo Especializado sobre el Crimen Organizado Transfronterizo¹⁹.

Lo expresado hasta aquí permite graficar la relevancia global del fenómeno de la cibercriminalidad, y de cómo todas las características tenidas en cuenta por el organismo de Naciones Unidas ya en 2010 -transnacionalidad de esta modalidad y su relación con el crimen organizado, necesidad de una legislación uniforme para una adecuada cooperación internacional y efectiva respuesta estatal- permanecen inalteradas en la actualidad.

III.- La evidencia digital en el proceso penal.

Resulta a esta altura evidente que la creciente utilización de las TIC's en casi todos los ámbitos de la vida de la sociedad moderna (comunicaciones y vínculos sociales, información contenida en archivos informáticos, comercio electrónico, diseños industriales, prensa y expresión de ideas, actividad bancaria, operaciones bursátiles, etc.) y la “revolución” que se ha producido en el área de las telecomunicaciones han generado un nuevo tipo de evidencia en los procesos penales, la *evidencia digital o electrónica*²⁰.

¹⁶Disponible en: <http://www.comjib.org/contenido/paises-iberoamericanos-firman-convenio-y-recomendacion-sobreciberdelincuencia-en-madrid>

¹⁷ Surgen de una decisión del Consejo del Mercado Común (CMC) del MERCOSUR N° 10/05 de fecha 19 de junio del año 2005, a raíz de la necesidad de contar con un mecanismo ágil en el relacionamiento entre los Miembros Públicos de los Estados Partes y Asociados, para lograr potenciar las acciones conjuntas para la prevención, investigación y represión del crimen organizado, narcotráfico y terrorismo, entre otros.

¹⁸Cfr. Los antecedentes de la XV REMPM celebrada en Montevideo, República Oriental del Uruguay, en 2013.

¹⁹Cfr. Los antecedentes de la VII REMPM celebrada en Asunción, República de Paraguay, en 2009)

²⁰ Para elaborarestecápite se consultaron, entre otros, los siguientes documentos: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice (NIJ), *Special Report, Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, disponible en: <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>; Association of Chief Police Officers (ACPO) from England, Wales & Ireland, *Good Practice Guide for Computer-Based Electronic Evidence, V. 4.0* disponible en: https://www.7safe.com/docs/default-source/default-document-library/acpo_guidelines_computer_evidence_v4_web.pdf;

U.S. Department of Homeland Security, United States Secret Service, *Best Practices for Seizing Electronics Evidence V.4.2*, disponible en <https://www.cwagweb.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf>

Prácticamente, en casi todos los procesos penales y mucho más en aquellos procesos denominados causas complejas (fraudes bancarios, infracciones al régimen penal cambiario y tributario, lavado de dinero, corrupción, etc.) en algún momento de la investigación es necesario recurrir a algún tipo de evidencia digital o electrónica (por ejemplo: archivos informáticos, comunicaciones electrónicas, ubicación geográfica de dispositivos de telecomunicaciones, datos de tráfico o de contenidos de comunicaciones, registros informáticos: tales como datos migratorios, bancarios, tributarios, etc.) ya que las TIC's han transformado substancialmente los procesos de intercambio de información y producción en todas las esferas de la vida.

Evidencia digital es cualquier información relevantes para una investigación obtenida a partir de un dispositivo electrónico o medio digital que sirve para adquirir convencimiento de la certeza de un hecho; en otros términos, es todo elemento probatorio cuya relevancia procesal depende del contenido del dato o de su particular localización en un dispositivo periférico determinado, o del hecho de haber sido transmitido mediante modalidad informática o telemática.

Así, la evidencia digital se denomina una “*slippery form of evidence*”²¹ (*forma resbaladiza de evidencia*), ya que presenta peculiaridades tales que ponen en entredicho su aplicabilidad a las disposiciones codificadas.

Pues, una de las características de la evidencia digital es su volatilidad. Esto conlleva a que la misma, por su propia naturaleza, sea frágil, fácil de alterar y dañar o, directamente, de destruir.

Para ello, téngase en cuenta que la fragilidad y la inmaterialidad son características intrínsecas del dato digital. En consecuencia, es fácilmente modificable, incluso debido a un simple acceso. Por tal razón, la protección de la autenticidad de la evidencia representa un aspecto absolutamente central de la cuestión, estrechamente vinculado al de la cristalización del *marco* informático a través de complejas operaciones técnicas y la trazabilidad de las operaciones realizadas en el mismo a través de la preparación de

²¹Cfr. Casey, Eoghan, *Digital Evidence and Computer Crime: Forensic science, computers and the Internet*, 3da. Edición, AcademicPress, abril 2011, pág. 15.

detallados *reports*, suficientemente idóneos como para evidenciar la denominada **cadena de custodia**(art. 157²² de CPPF).

Por tanto, la *evidencia digital* puede ser dañada o destruida, aunque de manera involuntaria, por alguien que no posea los conocimientos adecuados mientras va del investigador al consultor. Y esto es aún más grave dado que la partida se juega esencialmente fuera del debate, durante las investigaciones preliminares, y los intereses en juego son sumamente relevantes, garantizados constitucionalmente, como el derecho a la defensa.

Especialistas en informática forense la asimilan la *evidencia digitalo electrónica* al ADN o a las huellas dactilares por ser un tipo de prueba latente. Con esto nos estamos refiriendo a que dicha evidencia, en su estado natural, no nos deja entrever qué información es la que contiene en su interior, sino que resulta ineludible para ello, examinarla a través de instrumentos y procesos forenses específicos.

Por lo expuesto, resulta imperativo tomar precauciones especiales al momento de recolectar, manipular, documentar y examinar la *evidencia digitalo electrónica*, pues de lo contrario, dicho elemento probatorio puede tornarse inválido a los fines judiciales, o en su caso, mostrarse imprecisa a efectos de esclarecer el hecho delictivo.

Con todo, la *evidencia digitalo electrónica* se “obtiene” e “incorpora” al proceso penal a través del principio de libertad probatoria y sobre la base de aplicación analógica de reglas que regulan los medios de prueba tradicionales²³.

Algunos de los aspectos que hacen especial una investigación en entornos virtuales, son:

- El lugar de la acción del autor no coincide con el lugar de consumación del hecho. Así, la denominada *escena del delito* puede encontrarse en distintas jurisdicciones, convirtiéndose -generalmente- en un delito transnacional.

²² **CPPF 2018,Artículo 157.- Cadena de custodia.** “Con el fin de asegurar los elementos de prueba, se establecerá una cadena de custodia que resguardará su identidad, estado y conservación. Se identificará a todas las personas que hayan tomado contacto con esos elementos, siendo responsables los funcionarios públicos y particulares intervinientes”.

²³ Así, el Artículo 150 del CPPF que regula la *interceptación de correspondenciaelectrónica*o cualquier otra forma de comunicación establece, en su párrafo segundo, que:**Se procederá de modo análogo al allanamiento.**

A su turno, el Artículo 151 del CPPF, al regular la *Incautación de datos* dispone, en su párrafo segundo, que: **Regirán las mismas limitaciones dispuestas para el secuestro de documentos;** y, luego, en su párrafo cuarto, expresa: **Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia.**

- Uso durante el *itercriminis* de diferentes servidores; incluidos aquellos permiten el anonimato en las comunicaciones.
- Utilización de técnicas de encriptación
- Mínimo tiempo para la investigación y preservación de la *evidencia digitalo electrónica* por su fácil volatilidad y mutabilidad.
- Necesidad de contar con software de investigación y equipamientos tecnológicos idóneos -que difieren de acuerdo a las características del hecho- así como de conocimientos técnicos específicos de los operadores judiciales que tienen que obtener la *evidencia digitalo electrónica* y efectuar el analizar los elementos probatorios.

Por lo demás, es indispensable en algunas investigaciones, atendiendo a la *volatilidad* de las evidencias digitales o electrónicas, la preservación/aseguramiento rápido de datos informáticos almacenados *ya existentes* en algún soporte electrónico o digital de las comunicaciones y, en particular, de la dirección IP utilizada por el autor del hecho para poder identificarlo; especialmente, en aquellos supuestos en que los órganos de persecución penal tengan motivos para sospechar que los *datos de contenido* como los *datos de tráfico* pueden ser borrados o alterados²⁴.

Cabe destacar, que el CPPN²⁵ vigente no contiene ninguna norma que prevea estas situaciones.

III.1.- Pautas mínimas para recolección y preservación de evidencia digital o electrónica.

Entre las pautas mínimas que los investigadores deben observar en la recolección y preservación de la evidencia digital o electrónica durante todo el proceso, son:

(i) Al llegar a la escena del hecho donde se va a obtener evidencia digital o electrónica, se tiene que evitar su contaminación, retirando del lugar a toda persona ajena al procedimiento que se está desarrollando;

²⁴ Cfr. Artículo 16, inciso 1 y 2 del *Convenio sobre Ciberdelito*.

²⁵ El Código Procesal Penal de la Nación -vigente- fue aprobado por Ley N° 23.984 de fecha 21 de agosto de 1991; promulgado con fecha 04 de septiembre de 1991 y publicado con fecha 09 de septiembre de 1991.

- (ii) Ninguna acción de las fuerzas de seguridad o de los operadores judiciales debe alterar los datos contenidos en las computadoras o dispositivos de almacenamiento informático que luego serán utilizados como elementos probatorios;
- (iii) Si las circunstancias del caso hacen necesario que se deba acceder a los datos o información contenida en las computadoras o dispositivos de almacenamiento informático, la persona que efectúe dicha tarea debe ser idónea, es decir, contar con los conocimientos técnicos informáticos que la situación merece y, a su vez, capaz de explicar el motivo por el cual debió interactuar con la evidencia digital -por lo general, la urgencia del caso-, y los pasos llevados a cabo;
- (iv) Finalmente, se debe auditar y registrar fehacientemente todo el proceso relativo a la manipulación de la evidencia digital, precisando detalladamente las medidas y acciones llevadas a cabo, teniendo como eje central, la preservación de la cadena de custodia.

Un ejemplo que vulnera estas pautas mínimas, fue descripto por la Cámara Nacional de Apelaciones en lo Criminal y Correccional²⁶ al declarar inválida la actuación de las fuerzas de seguridad en un supuesto donde, aun cuando se trató de un celular hallado en poder del sospechoso, el preventor luego de incautarlo retiró su chip y lo colocó en el suyo, lo que puso en serio riesgo la prueba por la posible eliminación de información o, incluso, incorporación de otra. Ese procedimiento, por sus consecuencias irreproducibles, debió ser controlado por la defensa (art. 200 del Código Procesal Penal de la Nación).

En este caso, la jurisdicción hizo hincapié en los resguardos que se deben adoptar al manipularse prueba digital. Así, se sostuvo que “...desde el punto de vista de preservación de la evidencia digital, lo ideal es que la policía manipule lo menos posible los elementos informáticos, a fin de no alterar la información...”²⁷.

Pues, en este caso concreto, el preventor puso en riesgo la prueba obtenida. Incluso ese examen bien pudo afectar la intimidad del verdadero propietario ya que se accedió a información careciendo de autorización judicial para ello.

IV.- Las medidas de investigación tecnológica y sus principios rectores.

²⁶ Cfr. Cámara Nacional de Apelaciones en lo Criminal y Correccional, SALA 6, en causa N° 37.443/18, caratulada: *G., F. J. s/ nulidad*, resuelta el 31 de julio de 2018.

²⁷ Dupuy, Daniela-Kiefer, Mariana; “*Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*”; Euros Editores S.R.L, Buenos Aires, 2018, pág. 456.

El Código Procesal Nacional Federal²⁸ regula diferentes medios de investigación que, en mayor o menor medida, afectan al ámbito de los derechos fundamentales a la intimidad, la propia imagen, al secreto de las comunicaciones y a la protección de los datos personales garantizados por el artículo 18 de la Constitución Nacional.

Así, integran un catálogo -provisorio- de medidas de investigación tecnológica: i) la interceptación de las comunicaciones telefónicas y telemáticas²⁹; ii) el registro de dispositivos de almacenamiento masivo de información³⁰.

En tanto que: la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de

²⁸ El Código Procesal Penal Federal -en adelante, CPPF- fue aprobado por la Ley N° 27.063 y su texto fue ordenado según el Decreto N° 118/2019, publicado en el Boletín Oficial de fecha 8 de febrero de 2019 (conteniendo las incorporaciones dispuestas por la Ley N° 27.272 y las modificaciones introducidas por la Ley N° 27.482).

²⁹ Artículo 150.- **Interceptación.** Siempre que resulte útil para la comprobación del delito, *el juez podrá ordenar*, a petición de parte, **la interceptación** y secuestro de la correspondencia postal, telegráfica, **electrónica o cualquier otra forma de comunicación** o de todo otro efecto remitido por el imputado o destinado a éste, aunque sea bajo nombre supuesto.

Se procederá de modo análogo al allanamiento.

La **intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo máximo de treinta (30) días**, pudiendo ser renovada, expresando los motivos que justifican la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado.

La solicitud deberá indicar el plazo de duración que estime necesario según las circunstancias del caso. El juez controlará la legalidad y razonabilidad del requerimiento y resolverá fundadamente.

Rige para los magistrados, funcionarios, agentes y empleados que tengan participación activa en la intervención y/o responsabilidad sobre los elementos probatorios, el deber de confidencialidad y secreto respecto de la información obtenida por estos medios. Quienes incumplan este deber incurrirán en responsabilidad penal.

Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.

Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieren, hubiere transcurrido su plazo de duración o ésta hubiere alcanzado su objeto, deberá ser interrumpida inmediatamente.

³⁰ Artículo 151.- **Incautación de datos.** El juez podrá ordenar a requerimiento de parte y por auto fundado, el **registro de un sistema informático o de una parte de éste, 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**, bajo las condiciones establecidas en el artículo 136.

Regirán las mismas limitaciones dispuestas para el secuestro de documentos.

El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó.

Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia.

Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos.

seguimiento, localización y captación de la imagen; y, los registros remotos sobre equipos informáticos aún no han sido regulados en el CPPF.

Empero, como presupuesto indispensable para la adopción de cualquier medida de investigación tecnológica, es necesario establecer *en forma expresa* la necesidad de una *autorización jurisdiccional (emitida por juez)* dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida durante la investigación preparatoria del caso penal o, en ciertos supuestos, durante la fase de investigación pre-procesal.

En otras palabras, una medida de investigación tecnológica requiere la emisión de una resolución jurisdiccional motivada que contenga taxativamente los requisitos de proporcionalidad, racionalidad, necesidad y especialidad, como filtro de legalidad para la validez de cualquier medida de investigación limitativa de derechos fundamentales.

IV.1.- El principio de especialidad.

El principio de especialidad exige que una medida de investigación tecnológica se encuentre relacionada con la indagación de un delito concreto al menos en el plano indiciario, ya que puede modificarse posteriormente, por adición o suma de otras peculiaridades penales; por tanto, no pueden autorizarse medidas cuyo objeto consista en prevenir o descubrir delitos a ciegas o despejar sospechas sin una base objetiva.

La medida de investigación tecnológica tiene que delimitarse objetivamente mediante la descripción precisa del hecho que se trata de investigar y subjetivamente a través de la suficiente identificación del/los sospechosos, aportando no necesariamente la filiación completa de los sujetos afectados, aunque sí se requiere -al menos- indicar sus características físicas o datos indiciarios que permitan relacionarlos con el hecho investigado en el momento de adoptarse la medida de investigación tecnológica.

El principio de especialidad tampoco impone que se dé una identidad plena entre los hechos y sujetos investigados y los finalmente descubiertos ya que el objeto del proceso no responde a una imagen fija. Antes al contrario, se trata de un hecho de cristalización progresiva, con una delimitación objetiva y subjetiva que se verifica de forma paulatina, en función del resultado de las diversas diligencias probatorias³¹.

³¹ Cfr. Tribunal Supremo Español, Sala Segunda de lo Penal, STS N° 412/2011 de fecha 11 de mayo de 2011.

Supuesto distinto es la novación del objeto del procedimiento, es decir, cuando el delito que se descubre es otro diferente del concreto y determinado que justificó la adopción de la medida de investigación tecnológica. En estos casos se trataría de un supuesto de hallazgo casual y no existiría una infracción del principio de especialidad; y si los hechos conocidos aparentan una gravedad penal suficiente generaran una *notitiacriminis* que, siguiendo las normas de competencia territorial y temática, darán inicio a un nuevo caso penal.

IV.2.- El principio de idoneidad.

Toda resolución judicial que ordene la adopción de una medida de investigación tecnológica tendrá que valorar en *forma expresa* su aptitud potencial para la obtención de datos esenciales y de relevancia probatoria tanto en atención al objeto y sujeto investigado como -en su caso- a la duración de la medida.

IV.3.- Los principios de excepcionalidad y necesidad.

Existe una íntima relación entre los principios de excepcionalidad y necesidad³²; y, además, integran el principio de proporcionalidad. Cada principio interactúa a modo de esclusa del siguiente, de manera que la ausencia de cualquiera de ellos releva de la necesidad de examinar la pertinencia de la existencia de los restantes.

El principio de excepcionalidad posee un carácter general que tiene que ser complementado con el principio de necesidad mediante la ponderación específica de la medida de investigación tecnológica en relación con las circunstancias del caso en concreto.

En otras palabras, primero habrá que determinar que la medida de investigación tecnológica es idónea para la obtención de resultados relevantes para la investigación, para luego valorar si no puede adoptarse otra medida menos gravosa de forma que se entienda como necesaria en el caso concreto y, una vez superados estos filtros, analizar su

³² El principio de necesidad se encuentra indicado en el art. 11.2 de la Convención Americana de Derechos Humanos (en adelante CADH), cuando establece que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada; en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP); en el art. 8.2 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales (en adelante, CEDH), cuando prevé que la medida sea necesaria en una sociedad democrática; y en el art. 52.1 de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, CDFUE), que señala que sólo podrán introducirse limitaciones a estos derechos cuando sean necesarias.

proporcionalidad en sentido estricto. Pues, las medidas de investigación tecnológicas suponen un sacrificio para un derecho fundamental, lo que determina que el recurso a las mismas debe ser excepcional y no *rutinario*.

El vínculo existente entre ambos principios explica que el legislador haya querido definirlos conjuntamente a través de dos supuestos que pueden darse de manera alternativa, de forma que la concurrencia de cualquiera de ellos permitiría justificar el cumplimiento de ambos principios.

En suma, la autorización jurisdiccional de la medida de investigación tecnológica ha de justificar, en forma expresa, que los resultados que se pretenden obtener no puedan obtenerse mediante otras medidas menos invasivas respecto a los derechos fundamentales del investigado, medidas que, de esta forma, se convierten en imprescindibles desde la perspectiva del caso concreto.

IV.4.- El principio de proporcionalidad.

Las medidas de investigación tecnológica se consideran proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de la adopción de dichas medidas resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Así, la resolución jurisdiccional que autorice la realización de la medida de investigación tecnológica tendrá que exteriorizar los criterios seguidos y la ponderación de los intereses realizada.

La gravedad de la infracción tendrá que valorarse no sólo por la calificación de la pena legalmente prevista, sino que ponderando los bienes jurídicos protegidos y su relevancia social³³; y, además, en relación con la concreta limitación del derecho fundamental que comporte la medida de investigación tecnológica, ya que cuando la injerencia en el derecho no sea especialmente grave, la diligencia de investigación puede

³³ La incorporación de este particular criterio de ponderación reside en el hecho de que muchos de los delitos que se cometen mediante el uso de las TIC'S -y, considerando el alcance potencial del medio empleado- sólo pueden ser investigados a través de herramientas tecnológicas so pena de quedar impunes. Cfr. Tribunal Constitucional Español, Sala Primera, STC Nº 104/2006 de fecha 3 de abril de 2006.

estar justificada por el simple objetivo de prevenir, investigar, descubrir y perseguir infracciones no especialmente graves³⁴.

Finalmente, la relevancia del resultado perseguido con la restricción del derecho fundamental del investigado tiene que encontrarse vinculado directamente con los principios de idoneidad y necesidad y contendrá tanto la incidencia del descubrimiento en la integración y prueba de la correspondiente figura delictiva como el efecto de la medida en el restablecimiento de la paz social perturbada por el delito.

V.- Fortalecimiento de las garantías procesales

Para el fortalecimiento de las garantías procesales, en la regulación de las medidas de investigación tecnológica -indispensables para la investigación y persecución de las diversas formas delincuencia cibernética- se tienen que establecer *protocolos o guías específicas de adquisición de elementos procedimiento digitales o virtuales* para la correcta interceptación de las comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen; el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

Indudablemente, lastecnologías de la información y la comunicación (TIC's) se han convertido no sólo en una parte relevante de la vida de las personas, sino en el centro en torno al cual gravitan las diversas actividades en las sociedades modernas.

Ello también ha influido en el modo en el que se desarrollan numerosos comportamientos delictivos que, o bien recaen directamente sobre los dispositivos o sistemas informáticos, generando el nacimiento de nuevas formas de delito, o bien utilizan la informática como medio o instrumento privilegiado para su desarrollo.

Justamente por este motivo, en los últimos años, el uso de la informática ha resultado de capital importancia para la persecución del delito. Ambas circunstancias, además, constituyen el motivo esencial de la irrupción progresiva de la informática en el

³⁴ Cfr. En este sentido, véase Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de fecha 2 de octubre de 2018, asunto C-207/16.

proceso penal como objeto y medio de prueba y, al mismo tiempo, como medio de investigación de los delitos.

Así, se descarta que los dispositivos de almacenamiento masivo de información puedan ser considerados como simples piezas de convicción. Pues, su capacidad para recoger y conservar datos de muy diferente índole permite que el acceso a los mismos pueda llegar a afectar de manera intensa a diversos derechos fundamentales³⁵.

Al respecto, el artículo 19 del Convenio sobre la Ciberdelincuencia señala que: *“Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar: a) A un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio”*³⁶.

En el abordaje del registro de dispositivos o equipos informáticos, se tiene que distinguir entre:

- un registro estático, el correspondiente a los dispositivos de almacenamiento masivo de información; y,
- un registro dinámico, el registro remoto sobre equipos informáticos.

VI.- Los desafíos que genera el Derecho a la intimidad

³⁵ Esta idea, reconocida por la jurisprudencia, deriva de considerar a las PC's como algo más que un instrumento receptor de una serie de datos con mayor o menor relación con el derecho a la intimidad del usuario. Cfr. Tribunal Supremo Español, Sala Segunda en lo Penal, STS Nº 342/2013, de fecha 17 de abril de 2013.

³⁶ En el ámbito Europeo, la grave afectación de la intimidad que podía derivar del acceso sin consentimiento a datos informáticos almacenados ya había sido puesto de relieve en diversos instrumentos internacionales. Tal es el caso del Convenio Nº 108 del Consejo de Europa de fecha 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, disponible en: <https://rm.coe.int/16806c1abd>; la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de fecha 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) disponible en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32002L0058>.

En idéntico sentido, esta regulación legal del registro de dispositivos y sistemas informáticos era demandada por los Tribunales al resultar evidente la trascendencia que para la tutela de los derechos fundamentales podía suponer la protección del contenido almacenado. Cfr., en este sentido, Tribunal Constitucional de España, Sala Segunda en lo Penal, STC Nº 173/2011, de fecha 7 de noviembre de 2011.

En el ámbito de la Unión Europea³⁷, se encuentra en desarrollo jurisprudencialmente el concepto de “*derecho al entorno virtual*” como un derecho omnicomprendivo que abarca la protección de la gran diversidad de datos (agenda, con información acerca de hábitos personalísimos, mensajes de correo electrónico y mensajería instantánea, fotografías familiares, íntimas) que pueden guardarse en un dispositivo o sistema informático, como puede ser una computadora de escritorio, smartphones o teléfonos inteligentes.

Al respecto, el Tribunal Constitucional Español³⁸ ha sostenido que 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 virtual³⁹.

Así, el derecho al entorno virtual 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 públicos⁴⁰; generando la necesidad de dispensar una protección jurisdiccional frente a la necesidad del

³⁷ Cuya base normativa reside en el *Convenio N° 108 del Consejo de Europa sobre protección de los datos informatizados de carácter personal* (1981); las *Recomendaciones del Comité de Ministros* que lo desarrollan, en particular, la recomendación sobre datos personales utilizados en el sector policial (1987) y la recomendación sobre privacidad en Internet (1999), donde se pone de relieve que “el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las ‘autopistas de la información’ suponen riesgos para la intimidad de las personas naturales” y que “las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto a la intimidad y del secreto de las comunicaciones, tal y como se garantizan en el artículo 8 de la Convención Europea de los Derechos Humanos”. Además, recuerda que “el uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad” (introducción), por cuanto cada visita a un sitio de Internet deja una serie de “rastros electrónicos” que pueden utilizarse para establecer “un perfil de su persona y sus intereses” (apartado II, 2), subrayando también que la dirección de correo electrónico constituye “un dato de carácter personal que otras personas pueden querer utilizar para diferentes fines” (apartado II, 6).

³⁸ Cfr. Tribunal Constitucional de España, Sala Segunda, STS N° 173/2011 de fecha 7 de noviembre de 2011.

³⁹ Cfr. Tribunal Constitucional de España, Sala Segunda, STS N° 342/2013 de fecha 17 de abril de 2013.

⁴⁰ Cfr. Tribunal Constitucional de España, Sala Segunda, STS N° 342/2013 de fecha 17 de abril de 2013.

Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital.

Efectivamente, si estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, configuran un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona⁴¹.

El tratamiento unitario de los derechos comprometidos resulta necesario para garantizar la eficacia de un eventual registro, en atención a la gran diversidad de datos y archivos que pueden encontrarse en un dispositivo o sistema informático. Por ello, la autorización para el registro de un dispositivo o sistema informático en la que se habilite para el acceso a la totalidad del entorno virtual de su usuario, evitará que puedan surgir problemas derivados de la naturaleza del contenido que pudiera ser hallado.

Por su parte, el Tribunal de Justicia de la Unión Europea ha reafirmado la importancia del derecho a la protección de los datos personales como un elemento a tomar en consideración no sólo en el momento de transponer una directiva sino también cuando las autoridades estatales y los órganos judiciales nacionales procedan a su aplicación⁴².

En tanto que el Tribunal Europeo de Derechos Humanos ha venido asumiendo una interpretación extensiva del concepto “vida privada” del art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales. Así, considera que “el término ‘vida privada’ no se debe interpretar de forma restrictiva”, de forma que éste “engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes”, sin que “ninguna razón de principio permita excluir las actividades profesionales o comerciales”⁴³.

Específicamente, el TEDH considera que están incluidos en el ámbito de protección del art. 8 del Convenio europeo, por cuanto pueden contener datos sensibles que afecten a la intimidad, tanto “los correos electrónicos enviados desde el lugar del trabajo” como “la

⁴¹ Cfr. Tribunal Constitucional de España, Sala Segunda, STS N° 173/2011 de fecha 7 de noviembre de 2011.

⁴² Cfr. Sentencia del Tribunal de Justicia (Gran Sala) de 29 de enero de 2008, asunto C-275/06, Productores de Música de España (Promusicae) c. Telefónica de España, S.A.U., apartados 61-70.

⁴³ Cfr. TEDH, sentencia de fecha 16 de febrero de 2000, caso Amann contra Suiza, § 65.

información derivada del seguimiento del uso personal de Internet”⁴⁴. En este caso, precisa el Tribunal, a la demandante no se le advirtió de que podría ser objeto de un seguimiento, por lo que podía razonablemente esperar que se reconociera el carácter privado “en lo que respecta al correo electrónico y la navegación por Internet”⁴⁵.

De lo expuesto, se desprende que cualquier injerencia en el contenido de un computador personal -ya sea por vía de acceso remoto a través de medios técnicos, ya, como en el presente caso, por vía manual- deberá venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes otorgados por una resolución jurisdiccional.

La regulación legal encomienda ahora al juez valorar normalmente con carácter previo, aunque, en algunos supuestos con posterioridad al registro, la procedencia de la medida en el caso concreto, teniendo en cuenta que, con ella, los poderes públicos accederán a ese entorno virtual constitucionalmente protegido del que es titular el investigado. Por tanto, se sostuvo que 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 dispositivo⁴⁶.

Solo a la hora de motivar específicamente la medida deberá descenderse al análisis particular de los derechos controvertidos, cuyo mayor o menor protagonismo y afectación, determinarán la mayor o menor exigencia de los principios rectores que habrán de presidir la medida.

VII.- Colofón

Como se ha podido advertir, en el ámbito nacional, las medidas de investigación tecnológica requieren de una *reformulación* jurisprudencial sobre el alcance de las garantías procesales: especialmente, de la garantía de la intimidad.

⁴⁴ Cfr. TEDH, sentencia de fecha 3 de abril de 2007, caso Copland contra el Reino Unido, § 41.

⁴⁵ Cfr. TEDH, sentencia de fecha 3 de abril de 2007, caso Copland contra el Reino Unido, § 42.

⁴⁶ Cfr. Tribunal Supremo Español, Sala Segunda de lo Penal, STS N° 786/2015 de fecha 4 de diciembre de 2015.

Pues, en este tema, según entiendo, tampoco es conveniente la aplicación analógica de las normas vigentes ni es suficiente la construcción jurisprudencial de nuestro máximo tribunal en la interpretación de la garantía en su sentido clásico.

Antes bien, es conveniente un análisis de cada una de estas medidas de investigación tecnológicas tomando en consideración, para la regulación de las salvaguardas necesarias, su potencial de afectación del derecho a la intimidad conforme a los principios generales sentados en la jurisprudencia de los organismos europeos de Derechos Humanos.

Entiendo, además, que resulta cardinal regular en los códigos procesales penales medidas de investigación tecnológica destinadas a la investigación de los delitos que requieran la obtención de evidencia digital. En otras palabras, establecer normas especiales que consideren las características particulares que posee la investigación en entornos digitales.