Revista Brasileira de Direito Processual Penal
ISSN: 2525-510X
Revista Brasileira de Direito Processual Penal

Vadell, Lorenzo Mateo Bujosa; Rúa, Mónica María Bustamante; Garzón, Luis Orlando Toro
La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia
Revista Brasileira de Direito Processual Penal, vol. 7, núm. 2, i2.482, 2021
Revista Brasileira de Direito Processual Penal

DOI: https://doi.org/10.22197/rbdpp.v7i2.482

Disponible en: https://www.redalyc.org/articulo.oa?id=673972089016

La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia

Digital evidence resulting from covert surveillance: collection, admissibility and assessment in criminal proceedings in Spain and Colombia

Lorenzo Mateo Bujosa Vadell[1]

Universidad de Salamanca, Salamanca/Castilla y León, España

lbujosa@usal.es

http://orcid.org/0000-0003-1660-7483

Mónica María Bustamante Rúa[2]

Universidad de Medellín, Medellín/Antioquia, Colombia

mmbustamante@udem.edu.co

https://orcid.org/0000-0002-1029-1468

Luis Orlando Toro Garzón[3]

Universidad de Medellín, Medellín/Antioquia, Colombia

ltoro@udem.edu.co

http://orcid.org/0000-0002-3049-692X

[1] Universidad de Salamanca, Salamanca/ Castilla y León, España. Director del programa de Doctorado en Administración, Justicia y Hacienda en el Estado Social de la Universidad de Salamanca. Presidente del Instituto Iberoamericano de Derecho Procesal. Doctor en Derecho.

[2] Universidad de Medellín, Medellín/Antioquia, Colombia. Docente investigadora de la Facultad de Derecho. Directora de la Maestría en Derecho Procesal Contemporáneo. Integrante del Grupo de Investigaciones en Derecho Procesal. Investigadora Senior Minciencias. Doctora en Derecho.

[3] Docente investigador de la Facultad de Derecho de la Universidad de Medellín. Integrante del Grupo de Investigaciones en Derecho Procesal. Abogado. Doctor en Derecho Procesal Contemporáneo por la Universidad de Medellín.

Resumen: El artículo analiza algunas cuestiones problemáticas sobre la obtención, admisibilidad y valoración, en el proceso penal, de la prueba digital producto de la vigilancia secreta, en el marco de la era digital, desde una perspectiva comparada a partir de la experiencia española. Para ello, se presentan nociones y características de la prueba digital, y se plantean algunas problemáticas que representa este tipo de prueba en el proceso penal. Luego, se analizan las implicaciones de la obtención, admisibilidad y valoración de la prueba digital cuando ha sido producto de la vigilancia secreta. Finalmente, se presentan las reflexiones conclusivas sobre el tema.

Palabras clave: prueba digital; vigilancia secreta; admisibilidad probatoria; valoración de la prueba.

Abstract: *This article analyzes some problematic issues regarding the collection, admissibility and assessment in criminal proceedings of digital evidence resulting from covert surveillance, within the scope of the digital era, from a comparative perspective and based on the Spanish experience. To this end, some concepts and characteristics of the digital evidence are presented and some problems that this kind of evidence brings to criminal proceedings are presented. Then, the implications of how digital evidence is obtained, admitted and assessed when obtained by means of covert surveillance are analyzed. Finally, the concluding thoughts on the subject are presented.*

Keywords: *digital evidence; covert surveillance; evidential admissibility; evidence assessment.*

Introducción

El artículo aborda algunas cuestiones generales y problemáticas de la obtención, admisibilidad y valoración en el proceso penal de la prueba producto de la vigilancia secreta en la era digital, lo que resulta pertinente cuando se atiende a la experiencia española desde su marco normativo y desarrollo jurisprudencial, de cara a la necesidad de una mejor comprensión para los sistemas procesales como el colombiano, que no cuentan con una regulación concreta sobre la materia. Los objetivos del trabajo son: a) abordar la conceptualización y caracterización de la prueba digital en el proceso penal español, así como plantear los principales problemas que surgen en su producción; b) reflexionar sobre la obtención de la prueba digital a partir de la vigilancia secreta para finalmente, c) analizar algunos elementos para los juicios de admisibilidad y valoración probatoria de la prueba digital producto de la vigilancia secreta.

En el contexto del presente estudio, se aborda la vigilancia secreta con el enfoque de ser una actividad de investigación penal reservada, auxiliada por las tecnologías para la obtención de información probatoria en el ámbito procesal penal[4].

Se sigue una metodología cualitativa que parte del análisis de textos normativos de España sobre la prueba digital y la vigilancia secreta en el proceso penal. Igualmente, se realiza una exploración de la jurisprudencia española sobre los riesgos y limitaciones de la vigilancia secreta de cara a los derechos fundamentales en el proceso penal, para finalmente, triangular las ideas y reflexiones de algunos autores españoles sobre el tratamiento procesal penal y la eficacia probatoria de la prueba digital producto de la vigilancia secreta en el entorno virtual. Se parte de la siguiente pregunta: ¿cuáles son los elementos que se deben considerar

[4] En SALAMANCA AGUADO, E. El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones. *Revista del Instituto Español de Estudios Estratégicos (IEEE)*, n. 4. 2014. https://revista.ieee.es/article/view/306. Se desarrolla el concepto de captura masiva de información a través de programas secretos de vigilancia, y los efectos para los Derechos Humanos. El estudio se realiza a partir de la experiencia del Tribunal Europeo de Derechos Humanos, al resolver el asunto Big Brother Wath y otros contra Reino Unido.

en el juicio de admisibilidad y valoración probatoria de la prueba digital producto de la vigilancia secreta?

1. La prueba digital en el proceso penal

1.1 Conceptualización y caracterización de la prueba digital

Referirse a la prueba digital es abrirse a un universo de alternativas conceptuales desde el ámbito de la prueba, pues esta expresión está íntimamente ligada a los conceptos de prueba informática o electrónica y prueba tecnológica, sin desconocer otras denominaciones de singular importancia en el derecho probatorio por su amplitud polisémica, tal como la prueba cibernética, en esta se basa Díaz Limón, por acoger el concepto según el cual la cibernética es la ciencia que se encarga del estudio de la comunicación y el control entre el ser humano y la máquina[5].

La prueba digital puede estudiarse desde dos enfoques particulares: el primero está relacionado con la cualificación en la modalidad de prueba que es propia de aquella información cuya fuente es el ámbito digital, específicamente el soporte electrónico u ordenador, donde se genera por reacción electrónica de las máquinas o plataformas diseñadas para la producción o manejo de información inteligente, o por gestiones humanas con uso de mecanismos informáticos en correlación con las tecnologías de la información y las telecomunicaciones (TIC). El segundo orden o categoría probatoria se basa en el hecho mismo que surge o está almacenado en la fuente digital, con el que se pueden probar hechos de relevancia jurídica según su pertinencia, y sobre los cuales se fundan las relaciones o disputas de orden comercial, social, político o de reproche por comportamientos delictivos o contravencionales.

El hecho informático, obviamente, puede estar en canales privados o públicos, lo que hace complejo en menor o mayor grado la captación de tal información: es de poca complejidad cuando se cuenta con actos voluntarios de intercambio de comunicación y uno de los extremos de la

[5] DÍAZ LIMÓN, J. Incorporación de la prueba cibernética e informática: electrónica y digital. *Revista del Instituto Colombiano de Derecho Procesal*, n. 47, p. 23. 2018.

comunicación o los dos aportan los datos al proceso, o más complejo cuando se requieren mecanismos de investigación desarrollados jurídicamente para facilitar el acceso con diferentes fines, entre ellos el fin penal, este con un plus de complejidad por el aumento de restricciones a causa de su impacto en la intimidad como derecho supraordenado, según los presupuestos de protección y garantía convencional, constitucional y legal.

Los mecanismos de investigación, en su eficiencia y/o eficacia probatorias, dependen de protocolos comunes y de previsiones especiales por el escenario de comprometimiento digital en el que se da la gestión de búsqueda, identificación, fijación, recolección, embalaje, custodia y análisis de la información.

Estos, requieren de la correcta identificación e interpretación de los hechos en los medios de prueba clásicos, tales como la prueba documental y la prueba pericial, pero nada impide que bajo el ropaje del principio de libertad de la prueba los datos informáticos o digitales se presenten en un medio o instrumento independiente con denominación de prueba digital, prueba tecnológica o prueba telemática, o en algunos casos como documento electrónico por sus características diferenciales en cuanto a encriptamiento o forma codificada de la información que pueda tener, ello con relación al documento en general[6]. Ante este nuevo escenario probatorio sin duda el procedimiento investigativo debe ser adaptado, y así mismo bajo ese concepto de nueva clasificación es posible su admision, pues en nada se afecta el debido proceso, el derecho de defensa en particular, y la flexibilidad como variable en los diferentes contextos de la prueba, siempre y cuando se respete el núcleo esencial de garantías para las partes e intervinientes como la contradicción y la publicidad, y con las demás connotaciones esenciales antes anunciadas[7].

---

[6] Sobre la diferenciación del documento en general y el documento electrónico como fuente de prueba en particular, véase a CRUZ TEJADA, H. *La prueba documental electrónica frente al documento en soporte papel*. Nuevas tendencias del derecho probatorio. Bogotá: Ediciones Uniandes, segunda edición. 2015.

[7] Tal como se plantea en TORO GARZÓN, L.; BUSTAMANTE RÚA, M. La investigación y la prueba de contexto como elementos de política criminal para la persecución del crimen organizado. *Revista Criminalidad*, vol. 62, n. 1, p. 168, enero-abril. 2020. La tradición de los medios de prueba respecto de sus formas de producción, presentación, el protocolo de práctica y las reglas de

Así, el derecho de la prueba y a la prueba debe responder dinámicamente a los momentos evolutivos de la sociedad, y el desarrollo tecnológico es uno de estos contextos de mayor evolución en las últimas décadas, con incidencia plena en el comportamiento humano, por su recurrente tránsito a la interacción virtual.

Así lo destacan varios autores, al referirse por ejemplo a los documentos digitales o electrónicos que, dado al auge de los medios de comunicación digitales y producto de la denominada globalización electrónica, han adquirido una mayor importancia en la actualidad[8].

Como lo destaca Barreira, la comunicación se realiza en la actualidad, a través de variadas modalidades de mensajería, entre ellos los mensajes de texto, Whatsapp, Skype, Facetime[9]. A lo que ahora podríamos sumar otra cantidad representiva de aplicaciones como *Telegram y Signal*.

Adicional a ello, los sistemas de información y almacenamiento de la misma se transforman y actualizan en el día a día, como también el registro de los hechos se realiza cada vez con mayor frecuencia a través de variados medios digitales, en dispositivos móviles o a través de videocámaras ubicadas tanto en espacios públicos como privados.

El término digital aplicado a la prueba es consecuencia de la interacción de los actos del ser humano con la denominada era digital, que surge como hito de desarrollo en la tercera revolución industrial, sobre todo con la llegada de la electrónica y las TIC, lo cual se reconfigura a partir de la cuarta revolución industrial como tránsito a nuevas tecnologías, con pleno aporte de los seres humanos en su desarrollo y vinculación global desde el uso de nuevos conceptos de intercambio digital de actos sociales, servicios y productos.

---

valoración son circunstancias de constante debate por los cambios necesarios en la dinámica interpretativa y adaptativa que requiere el derecho según la evolución social.

8 ACEVEDO SURMAY, D.; GÓMEZ USTARIS, É. Los documentos electrónicos y su valor probatorio en procesos de carácter judicial. *Iustita. Revista de la División de Ciencias Jurídicas y Políticas*, n. 9, p. 391–419. 2011. https://doi.org/10.15332/iust.v0i9.905

9 BARREIRA, M. V. Impacto de las nuevas tecnologías en la prueba judicial civil. *Revista de Derecho de la Universidad de Montevideo*, n. 37, p. 139-176. 2020. https://doi.org/10.47274/DERUM/37.7

Al referenciar las expresiones prueba tecnológica, prueba electrónica y prueba digital, Arrabal Platero, orienta su postura diferenciadora en cuanto a la prueba digital, adhiriendose a la definición adoptada en el diccionario de la Real Academia Española, según la cual, *digital* es "un aparato o sistema que presenta información mediante el uso de señales discretas en forma de números o letras", de ahí que, para la investigadora, solo sería prueba digital cuando el dato se presente en códigos binarios[10]. Al respecto, en un ámbito de doctrina compartida y tras la ruta de diferenciar el documento electrónico del documento digital, Díaz Limón adopta el concepto del Diccionario *Legal Black* en cuanto a que lo digital son datos enviados en código de encendido y apagado representados por 1-0 (código binario)[11]. Sin embargo, el propósito del presente estudio no es centrarse en dicha diferenciación, por más que se considere aceptable desde el punto de vista temático, pues su título está relacionado en general con la información que se capta en o a través de los medios de vigilancia secreta en el orden informático o digital con relevancia para el proceso penal.

1.2 Problemas de la prueba digital en el proceso penal

El derecho penal contemporáneo, a pesar de acoger y conservar en gran medida los lineamientos sustanciales clásicos y la filosofía jurídica que le orientan, se ve, por una parte, exigido a actualizar como estrategia de política criminal el catálogo de injustos penales y de penas ante las nuevas formas, métodos y espacios de criminalidad. De otro lado, se ve ampliamente comprometido desde el proceso como escenario de articulación de las instituciones jurídicas, a actuar en medio de las

---

[10] ARRABAL PLATERO, P. *Tratamiento procesal de la prueba tecnológica*. Tesis (Doctorado en Ciencias Sociales y Jurídicas). Universidad Miguel Hernández, Madrid. 2019, p.4.

[11] El autor se apoya en las tesis del doctor Julio Téllez Valdés (*Derecho Informático*. Cuarta Edición. México: Ed. McGrawhill, 2009) sobre la aceptación de un término genérico de documento informático, para evitar hablar de documento electrónico o documento digital. DÍAZ LIMÓN, J. Incorporación de la prueba cibernética e informática: electrónica y digital. *Revista del Instituto Colombiano de Derecho Procesal*, n. 47, p. 23. 2018.

encrucijadas que se generan por la incidencia procesal de las garantías de orden convencional y constitucional, a modernizar y ejecutar nuevas metodologías e instrumentos de investigación, máxime en los tiempos actuales en que la denominada cibercriminalidad y otros focos de desestabilización traen consigo nuevos paradigmas o retos de justicia.

Sumado a ello, en la práctica judicial se debe evitar el accionar discrecional por ausencia de regulaciones precisas, pues esto puede derivar en actuaciones investigativas injustas, tal como lo plantean desde la experiencia de Chile, Viollier Bonvin y Ortega Romo, al analizar las consecuencias de ilicitud probatoria en la denominada *operación Huracán*, en cuanto a la interceptación de mensajería instantánea o la utilización de software maliciosos (malware o técnicas phishing) en la actividad de inteligencia policial, al denotar el interrogante: "¿hasta qué punto se ajusta a nuestro ordenamiento jurídico la utilización de técnicas de hacking en el contexto de la persecución penal y la labor de inteligencia?", emitiendo como respuesta: "así, tanto los derechos y garantías fundamentales como eventuales afectaciones no son absolutas, por lo que, se requiere una adecuada ponderación", respuesta que armonizan con el criterio de que: "el principio de reserva legal establece que las medidas intrusivas solo pueden ser hechas en la forma y condiciones específicamente establecidas por la ley"[12].

En ese sentido, son diversas las fronteras de carácter sustancial, procesal y específicamente probatorias que se deben estudiar para contar con respuestas oportunas y calificadas en la nueva justicia penal. Esta denominación se asume en el entendido de actuaciones de orden punitivo aplicadas en situaciones especiales por su complejidad e impacto, entre las que resaltan los crímenes de contexto, crímenes de organización y/o crímenes de acción y afectación tecnológica o digital. En ese panorama, el derecho probatorio penal debe reinventarse para determinar los medios y cauces más técnicos para gobernar tales hechos.

Entre los hechos de novedad penal, llama la atención respecto del presente escrito, los hechos digitales, que, por su naturaleza especial,

---

[12] VIOLLIER BONVIN, P.; ORTEGA ROMO, V. Cuando el Estado Hackea: El caso de operación Huracán. *Revista Chilena de Derecho y Tecnología*, v. 8, n. 2, p. 83-110. 2019.

comprometen la seguridad y la convivencia, acontecer que se presenta por la oportunidad para el delito que se genera con el tráfico masivo de datos a través de internet en las redes sociales y otras aplicaciones en diferentes órdenes de interacción humana. La calificación de especial se funda en la metodología delictual, las características del delito, el espacio de comisión, y en los intereses que se ponen en riesgo con las interacciones electrónicas y su aumento desaforado. De ahí, que, evidenciar estos hechos con instrumentos y actuaciones técnico-científicas, a la par del desarrollo tecnológico, puede ser problemático si las regulaciones normativas para la actuación investigativa y de juicio penal no son precisas, si la experiencia para su uso y administración es reducida, si la armonía en las actuaciones no se consigue, si la confianza en la autoridad judicial es limitada o si la logística tecnológica no cuenta con los desarrollos y ajustes necesarios en relación con las garantías procesales precisadas en la jurisprudencia nacional o internacional.

En cuanto al déficit de regulación normativa, Armenta Deu precisa, a partir de la experiencia en España, sobre la obsoleta regulación en las actuaciones jurisdiccionales, respecto de la protección de datos generados por el tratamiento de los dispositivos de almacenamiento masivo, y asegura que, el artículo 579 de la Ley de Enjuiciamiento Criminal (LECrim) fue aplicado analógicamente hasta 2015 para afrontar la legalidad de actuaciones en el panorama criminal con impacto social complejo[13], denotando como positiva la reforma legislativa producida a partir del año 2015, pues esta mitiga la injusticia normativa advertida por el derecho internacional de los derechos humanos y la jurisprudencia interpretativa de orden supranacional.

Para la autora, la investigación tecnológica a partir del ajuste normativo en España se ubica en dos fuentes, a saber*:* "los procesos comunicativos y los dispositivos y sistemas informáticos de almacenamiento de datos", y exalta como acertado el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta situación debe ocurrir en igual sentido en Colombia, donde la aplicación

[13] ARMENTA DEU, T. Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre. *Revista de Internet, Derecho y Política*, n. 27, p. 69. 2018.

de la Ley 906 de 2004, en lo referente a las actuaciones investigativas en general, se extiende a las situaciones de ocurrencia tecnológica por analogía normativa.

En cuanto a la experiencia en la administración de justicia en el entorno digital, la Corte Constitucional colombiana, al analizar la constitucionalidad del Decreto Legislativo 806 de 2020 (por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en el ámbito judicial), en la Sentencia C-420 de 2006, referente a la estabilidad y cobertura de la justicia digital, adujo que: "esta no es inmediata. Por el contrario, requiere de un proceso de adaptación progresiva de parte de la administración, los usuarios y funcionarios judiciales"[14]. Tiempo y forma que, de permitirse en exceso en el caso penal, posibilitarían el amparo irrazonable a quien delinque y la denegación de justicia para las víctimas y la sociedad.

Respecto de los derechos y garantías procesales de carácter constitucional, es evidente que estos pueden ser límite a la eficacia de la prueba construida en entornos digitales, por ello, cualquier actuación orientada a conseguir o asegurar información de esta naturaleza con relevancia para el derecho procesal, penal debe pasar por el tamiz de control de legalidad en los diferentes ciclos de gestión judicial, es decir, deben existir el autocontrol en la Policía Judicial y la Fiscalía o en sus similares en el ámbito nacional o internacional, activismo del juez de control de garantías u órgano encargado de tal función con posibilidad de exclusión de información probatoria en forma extendida y, por supuesto, control superlativo del juez en funciones de conocimiento para impedir el ingreso o valoración de información que no cumpla con estos presupuestos de garantía.

A este control de legalidad, le son aplicables en adición esencial los criterios elaborados por la Corte Constitucional[15], en cuanto a aplicar el método de ponderación para determinar en justo balance si la medida o actuación investigativa que se dispone o solicita "reúne las condiciones

---

[14] Corte Constitucional de Colombia, Sentencia C-420. M. P. (E). Dr. Richard Ramírez Grisales. 24 de septiembre de 2020.

[15] La Corte Constitucional es el órgano jurisdiccional instituido como máximo juez en Colombia, encargado de la salvaguarda y la interpretación de la supremacía constitucional.

de idoneidad, necesidad y proporcionalidad en el caso concreto"[16]. Estos criterios fueron elaborados como regla jurídica después de interpretar las diferentes posturas de orden nacional e internacional, en cuanto a la afectación de la intimidad personal corporal, y la privacidad en el uso y goce de la vida familiar y de bienes del investigado o imputado penal, en el ejercicio de los actos de investigación penal.

Algunas actuaciones investigativas que se resaltan doctrinalmente son: el cateo o registro informático descrito por Campoli[17], la vigilancia masiva de comunicaciones descrita por Salamanca Aguado[18], el agente informático como técnica especial de investigación en la lucha contra el crimen organizado (denominado también punitivismo infiltrado), las escuchas e interceptación de comunicaciones, la vigilancia con cámaras, los seguimientos pasivos, los "*entrampamientos*", las técnicas de recuperación de datos y las actuaciones bajo identidad supuesta. Del estudio y análisis de estas técnicas se ocupa en forma brillante Escalante Barreto [19], en un claro contraste entre la realidad del cibercrimen en sus diferentes focos o modalidades, los derechos y garantías constitucionales y la obligación del Estado de perseguir y develar el crimen de ocurrencia virtual.

Este enfoque de técnicas de investigación, con compromiso de fuentes informáticas, se agrupa en la denominada informática criminalística, de la cual se indica que es una disciplina acompañada de técnicas especiales para identificar y seguir las huellas y evidencias digitales. Entre estos focos digitales se ubican el video digital, el audio digital, la imagen digital y la informática forense. El nacimiento de esta disciplina de orden tecnológico se ubica en el año 1999 por la incidencia de las nuevas tecnologías de la información y la comunicación en el

---

[16] Corte Constitucional de Colombia, Sentencia C-822. M. P. Manuel José Cepeda Espinosa. 10 de agosto de 2005.

[17] CAMPOLI, G. A. *Manual Básico de Cateo y Aseguramiento de Evidencia Digital*. Bogotá: vLex International, n. 14, mayo. 2013.

[18] SALAMANCA AGUADO, E. El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones. *Revista del Instituto Español de Estudios Estratégicos (IEEE)*, n. 4. 2014.

[19] ESCALANTE BARRETO, E. *El agente encubierto informático como Técnica Especial de Investigación en la lucha contra el crimen organizado*. Bogotá: vLex International, n. 48, julio. 2019.

crimen[20]. Igualmente, se acoge por parte de los autores antes citados, el criterio de (Rodriguez *et al*., 2011), en cuanto a que la informática criminalística es: "un proceso metodológico para la recogida y el análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales".

2. Obtención de la prueba digital a partir de la vigilancia secreta en el proceso penal

Los actos de investigación penal que comprometan los derechos fundamentales por efecto de la innovación e impacto en la vida cotidiana de los nuevos desarrollos tecnológicos, deben estar fundados en el principio de legalidad, de ello se deriva que la ley: "debe precisar todas y cada uno de los presupuestos y condiciones de la intervención"[21] y no dejar a discrecionalidad de los investigadores y los jueces la interpretación en particular de los intereses y garantías prevalentes en cada caso de búsqueda o recolección de evidencia incriminatoria.

La reforma operada en España por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica[22], supera una larga etapa de insuficiencia normativa respecto a la aplicación de la nueva tecnología para la investigación de infracciones criminales. En efecto, la carencia de una regulación sistemática, incluso de la tan utilizada interceptación de comunicaciones telefónicas, dio lugar a repetidas condenas a este país por el Tribunal Europeo de

---

[20] NARANJO GÓMEZ, B.; MENDOZA PÉREZ, J.; ALONSO BETANCOURT, E.; HINOJOZA CALZADA, J. Informática criminalística: una especialidad en desarrollo. *Opinión Jurídica,* vol. 19, n. 38, p. 245-257, ene-jun. 2020.

[21] En LOPEZ BARAJAS PEREA, I. Garantías Constitucionales en la Investigación Tecnológica del delito: previsión legal y calidad de la Ley. Revista de Derecho Político, Madrid, n. 98, enero-abril, p. 11. 2017, se cita la sentencia TJUE del 08 de abril de 2014, apartado 47-54, sobre las precisiones que debe tener la ley para la autorización de las investigaciones del delito en el orden tecnológico en función de las garantías constitucionales.

[22] Boletín Oficial del Estado (BOE) n.° 239, de 6 de octubre de 2015.

Derechos Humanos (TEDH)[23] y fue voluntariosamente suplida por la jurisprudencia de la Sala Segunda del Tribunal Supremo[24]. Por ello, esta reforma supuso un considerable avance, pues no solo procedió a introducir la regulación supranacionalmente exigida, sino que introdujo nuevas formas de investigación penal que contrastan aún más con la ancianidad del continente, nuestra venerable Ley de Enjuiciamiento Criminal de 1882.

El legislador tuvo el cuidado de establecer numerosas garantías y consideraciones de proporcionalidad para la aplicación también de las interceptaciones de comunicaciones telemáticas, para la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, para la utilización de dispositivos de seguimiento, localización y captación de la imagen[25], para el registro de dispositivos de almacenamiento masivo de información y para la realización de registros remotos sobre equipos informáticos (arts. 588 bis a 588 *octies)*, que a su vez fueron objeto de estudio por cinco circulares de la Fiscalía General del Estado y que, en realidad, componen un cuerpo interpretativo único, aunque fragmentado[26].

---

[23] Así, en el *Caso Valenzuela Contreras contra España* (Sentencia de 30 de julio de 1998) y en el *Caso Prado Bugallo contra España* (Sentencia de 18 de febrero de 2003), por los que el Tribunal Europeo entendió que, a pesar de algunas reformas normativas, la regulación española no cumplía adecuadamente las exigencias de la jurisprudencia europea, básicamente "la determinación de las infracciones que pudieran dar lugar a las escuchas, la fijación de un límite a la duración de la aplicación de la medida y las condiciones para extender las actas de síntesis consignando las conversaciones interceptadas, tarea que es dejada en exclusiva al secretario judicial del tribunal. Las insuficiencias se refieren también a las precauciones a tomar para comunicar las grabaciones realizadas, intactas y completas, a fin de que pueda procederse a un control por el juez y por la defensa. La ley no contiene disposición alguna a este respecto". STEDH de 18 de febrero de 2003. §30.

[24] Especialmente por la Sentencia del Tribunal Supremo (STS), Sala 2.ª, de lo Penal, de 18 de julio de 1982.

[25] Llama la atención la referencia normativa a la funcionalidad de las medidas y no a la mención de los determinados dispositivos que puedan utilizarse. Con ello vemos clara la intención del legislador de prever una regulación lo más amplia posible en la que quepan instrumentos que todavía al día de hoy no se han desarrollado. Cfr. BUENO DE MATA, F. *Las diligencias de investigación en la cuarta revolución industrial. Principios teóricos y problemas prácticos*. Madrid: Aranzadi, Cizur Menor. 2019, p. 126.

[26] Circular 1/2019, de 6 de marzo, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de

Como se aprecia fácilmente, con ello el proceso penal español se beneficia de un amplio abanico de posibilidades de vigilancia secreta, de la que es posible obtener fuentes de prueba a través de normas procedimentales novedosas, encabezadas por unas disposiciones comunes de gran importancia, pues son las que disponen con carácter general los pormenores sobre la adquisición de ese material probatorio. Fuera de ellas, caeremos en el cenagoso ámbito de la prueba ilícita[27] y, por tanto, como mínimo en la inutilidad, y tal vez también en conductas tipificadas en las normas penales[28].

Es destacable el contenido de estas normas de aplicación general (arts. 588 bis a 588 bis b), que son un excelente ejemplo normativo de los parámetros de proporcionalidad, empezando por la aplicación, salvo excepciones[29], del criterio de la autorización judicial previa. Se pretende, además, evitar la utilización de estas medidas de manera generalizada o

---

Enjuiciamiento Criminal; Circular 2/2019, de 6 de marzo, sobre interceptación de comunicaciones telefónicas y telemáticas; Circular 3/2019, de 6 de marzo, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; Circular 4/2019, de 6 de marzo, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; y Circular 5/2019, de 6 de marzo, sobre registro de dispositivos y equipos informáticos.

27 Ténganse en cuenta, sin embargo, las interpretaciones restrictivas ahora dominantes sobre esta materia. Véase: ASENCIO MELLADO, J. M. La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita. *Diario La Ley*, n. 9499. 2019.

28 Así, por ejemplo, el artículo 197.1 del Código Penal de España establece que: "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

29 Así, el artículo 588 *quinquies* LECrim permite a la policía judicial la obtención y grabación "por cualquier medio técnico [de] imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos", pudiendo afectar también a "personas diferentes al investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación".

para investigaciones abstractas, lo que con frecuencia se conoce como "inquisitiones generales"[30]. Deben aplicarse, por tanto, consideraciones concretas respecto a la investigación de cada infracción criminal definida por unas coordinadas espacio-temporales concretas. No cabe, por tanto, utilizar estas medidas para investigaciones prospectivas, ni siquiera para la prevención de delitos. Es preciso delimitar el ámbito objetivo y subjetivo, además de la duración de la medida. En virtud de su utilidad: debe ser adecuada para obtener datos relativos a la comprobación de los hechos y/o para la averiguación de los delincuentes, pero para los hechos concretos y los sospechosos implicados en ellos.

La excepcionalidad y la necesidad son reguladas de forma conjunta y puestas en relación con la existencia o no de otras medidas menos gravosas para los derechos fundamentales del sujeto pasivo de la investigación, e igualmente útiles para el esclarecimiento del hecho o, cuando sin la aplicación de la medida de que se trate, para el descubrimiento o comprobación del hecho concreto, la determinación del autor o autores, la averiguación de su paradero o la localización de los efectos del delito se prevea que se van a ver dificultadas. Se erige una dificultad grave[31]. Por otro lado, la necesidad resalta una comparación: dada la situación excepcional en la que se encuentre el juez de instrucción, sólo podrá decidir adoptar alguna de estas medidas si no hay otras vías menos restrictivas de los derechos implicados, pero igualmente efectivas[32]. En definitiva, en el ámbito de la investigación penal es la limitación razonable de los derechos fundamentales, dentro de lo permisible para una sociedad democrática, si se quiere utilizar la expresión común en el sistema europeo de protección

---

30 AGUILERA MORALES, M. *Proceso penal y causa general en el Derecho español*. Madrid: Aranzadi-Civitas-Thomson Reuters. 2008.

31 No podemos perder de vista que "no estar localizado de manera continua es un derecho" o también que "la geolocalización supone una injerencia en la privacidad". VELASCO NÚÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*. Madrid: Sepin. 2016.

32 Así, la STS, Sala 2.ª, de lo Penal, de 30 de octubre de 2020, sobre el asesinato de un paciente en un hospital: "La colocación de cámaras de vigilancia en el pasillo de distribución a las habitaciones del hospital, es una medida que invade de forma menos trascedente la intimidad de las personas, pues no se afectan lugares de mayor intensidad, lo que precisaría una mayor exigencia en el control de su necesidad".

de derechos humanos y libertades fundamentales. Así, para considerar proporcionadas las diligencias es preciso tomar en consideración todas las circunstancias concurrentes y valorar el sacrificio de los derechos e intereses afectados, para que la afección no sea superior al beneficio que pueda aportar al interés público y de terceros[33].

A la regulación común se añaden unos presupuestos concretos que se deben sumar a las consideraciones generales y que todavía, con buen criterio, restringen más la aplicabilidad de estas medidas. Así, respecto a la interceptación de las comunicaciones telefónicas y telemáticas se establece una concreción, no tanto de proporcionalidad sino de afinidad material: no es solo la gravedad de los hechos lo que hay que tener en cuenta como base de la aplicación de estas medidas, sino también que se trate de delitos cometidos en el seno de un grupo u organización criminal o delitos de terrorismo, o que se hayan cometido a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación[34].

Expresamente, no se establecen presupuestos específicos cuando se trata de la captación de la imagen o de la utilización de dispositivos técnicos de seguimiento y de localización, ni respecto al registro de dispositivos de almacenamiento masivo de información, otra cosa es que se exijan unas bases materiales específicas o se establezca la "necesidad de una motivación individualizada". Sí se prevén esos presupuestos de manera explícita cuando se regula la posibilidad de registros remotos sobre equipos informáticos y se limita a cinco categorías de delitos, algunos de ellos no previstos en los casos anteriores: delitos cometidos en el seno

---

[33] Es interesante, además, que ofrezcan criterios para esta ponderación, con lo que cambia una larga tendencia del legislador que traspasaba indebidamente al juzgador la fijación de las bases principales para las limitaciones. Aunque todavía parece criticable que se pida atender a la trascendencia social de la medida —si por ello se entienden sus efectos en la opinión social—, sobre todo si tenemos en cuenta que la masa social es manejada por abundantes medios de comunicación morbosos y amarillistas, con lo que el criterio de razonabilidad podría desviarse hacia derroteros ajenos a los fines constitucionalizados.

[34] Véase RODRÍGUEZ ÁLVAREZ, A. Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal. En: ASENCIO MELLADO, J. M. (Dir.). *Justicia penal y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch. 2017.

de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional y, finalmente, delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

Se establece la posibilidad de que la adopción de las medidas que afecten a derechos fundamentales se haga de oficio o a instancia de la Fiscalía o de la Policía Judicial, a partir de solicitudes en las que se pormenoricen los datos necesarios para las consideraciones de proporcionalidad a las que ya se ha hecho alusión. Todo ello implicará una decisión judicial tomada en secreto[35] y en un plazo muy corto (de veinticuatro horas). No olvidemos que se trata de investigar hechos que están ocurriendo o que están a punto de ocurrir y que la demora podría convertir en inefectivas tales medidas[36]. Se trata de combinar, una vez más, la eficacia con una suficiente garantía en la adopción de la decisión que corresponda, según la concreción de las valoraciones que haga el juez de instrucción sobre las bases fácticas que tenga para decidir[37]. Estamos ante

---

[35] Conforme al artículo 588 bis d. Secreto. de la LECrim: "La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa", es decir, sin necesidad de aplicar la disposición más general del párrafo segundo del artículo 302 de la LECrim: "No obstante, si el delito fuere público, podrá el Juez de Instrucción, a propuesta del Ministerio Fiscal, de cualquiera de las partes personadas o de oficio, declararlo, mediante auto, total o parcialmente secreto para todas las partes personadas, por tiempo no superior a un mes cuando resulte necesario para: a) evitar un riesgo grave para la vida, libertad o integridad física de otra persona; o b) prevenir una situación que pueda comprometer de forma grave el resultado de la investigación o del proceso".

[36] De todas formas, el propio legislador ha introducido una razonable previsión de suspensión de ese breve plazo en caso de necesitar ampliación de datos o aclaración de los términos de la solicitud.

[37] También es cauto el legislador al encauzar el contenido de la resolución judicial, pues según el apartado tercero del artículo 588 bis c. LECrim debe determinar: "a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida. b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido. c) La extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a. d) La unidad investigadora de

decisiones en las que la privacidad de los individuos indiscutiblemente se ve afectada[38] y se plantea la llamada "expectativa razonable de privacidad" para contribuir a fijar sus límites[39].

La duración de la medida adoptada deberá limitarse al tiempo imprescindible para el esclarecimiento de los hechos. No cabe olvidar la excepcionalidad y la prioridad de los derechos fundamentales, que ofrecen un claro criterio interpretativo. Además, la provisionalidad de su adopción también caracteriza transversalmente esta aplicación: se debe acordar el cese de la medida "cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de esta no se están obteniendo los resultados pretendidos"[40].

En cualquiera de los casos, el control jurisdiccional de la medida es fundamental y eso exige que la Policía Judicial informe al juez de instrucción o de control de garantías competente del desarrollo y de los resultados obtenidos. Para ello, la resolución de autorización debe establecer la forma y periodicidad de esta comunicación. Y, desde luego, la información obtenida está destinada a la investigación dirigida a la comprobación de los hechos y la averiguación de los delincuentes, por ello, cuando acabe la intervención, cualquiera que sea la causa de esta finalización, deben transmitirse los resultados al órgano encargado de tal investigación[41].

Policía Judicial que se hará cargo de la intervención. e) La duración de la medida. f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida. g) La finalidad perseguida con la medida. h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia".

38 Incluso respecto a casos de geolocalización, el Tribunal Supremo de los Estados Unidos ha considerado que los controles a través de GPS sin autorización judicial constituyen violaciones a la Cuarta Enmienda. Véase: MOENSSENS, A. A.; DESPORTES, B. L.; EDWARDS, C. N. *Scientific Evidence in Civil and Criminal Cases*. New York: Foundation Press, 2013, pp. 236-237.

39 Véase RODRÍGUEZ LAINZ, J. L. "La nueva jurisprudencia sobre dispositivos de seguimiento y localización (Comentario a la STS, Sala 2.ª,141/2020, de 13 de mayo)". *Diario La Ley,* n.° 9650, 10 de junio de 2020.

40 Art. 588 bis j. de la LECrim.

41 Sobre el control *ex post,* véase DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: Ed. La Ley, 2016, pp. 355-356.

Se permite expresamente que lo obtenido en estas investigaciones pueda ser utilizado como "medio de investigación o prueba en otro proceso penal", y para ello se deducirá testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. El juez competente para el nuevo proceso deberá autorizar o no la continuación de la medida sobre el nuevo delito descubierto tras la valoración de las circunstancias fácticas, con decisión expresa sobre el secreto de las actuaciones[42].

3. Admisibilidad y valoración de la prueba digital producto de la vigilancia secreta

3.1 Aspectos generales

En el proceso penal, la prueba digital atraviesa por las fases de obtención de la información o datos, la incorporación de los datos al proceso y la valoración de los datos incorporados[43]. En el proceso penal español y colombiano, la investigación se encomienda al Ministerio Fiscal en el proceso de menores y al juez de instrucción en el proceso de adultos, en España, y a la Fiscalía General de la Nación en Colombia, que tienen la tarea de coordinación técnico-científica de las autoridades de policía judicial y con el control de un juez. Resulta cada vez más frecuente la incautación de equipos informáticos o de dispositivos de almacenamiento de datos[44] o el registro y la vigilancia secreta a través de estos medios, y es realmente relevante el contenido de los mismos que llega al proceso penal a través del reconocimiento del investigado, la declaración de testigos (incluidos el investigador de campo y el informático como testigos de acreditación) o a través de un dictamen pericial informático que debe ir acompañado del testigo experto (la declaración del perito informático).

---

[42] En el trasfondo, surge un problema acerca del tratamiento de datos personales que en Europa ha sido objeto de gran atención jurídica en los últimos años y se ha elevado a la categoría de derecho fundamental. Cfr. la Directiva 2016/680, del 27 de abril de 2016 [DOUEL 119/89 de 4 de mayo de 2016].

[43] DELGADO MARTÍN Joaquín. La valoración de la prueba digital. *Diario La Ley,* N.° 6, Sección Ciberderecho, Madrid: Ed. Wolters Kluwer, 2017.

[44] ABEL LLUCH, Xavier; RICHARD GONZÁLEZ, Manuel. *Estudios sobre la Prueba Penal.* Madrid: Ed. La Ley, 2013.

De la Torre Rodriguez se refiere a la prueba digital como: a) cualquier información digital; b) la información que es producida, almacenada o transmitida por medios digitales; c) información susceptible de tener el efecto de acreditar hechos en un proceso judicial, y d) se trata de una categoría de prueba tecnológica. Asimismo, caracteriza la prueba digital como:

- *Intangible:* dado que solo puede apreciarse a través de complejos procesos informáticos.
- *Replicable:* en tanto se puede copiar o replicar tantas veces se desee. Lo que plantea un problema de identificación de originalidad.
- *Volátil o mudable:* porque es inconstante por su naturaleza intangible. Sujeta a posibilidad de modificación o alteración.
- *Deleble:* dado que puede ser fácilmente destruida, aunque se conserve el soporte digital.
- *Parcial:* en ocasiones, la prueba digital está formada por múltiples ficheros informáticos repartidos en diferentes soportes digitales y localizaciones, lo que hace más compleja su aprehensión y preservación[45].

En este escenario, es fundamental acreditar la autenticidad e integridad de la fuente de prueba a través de las reglas de cadena de custodia. Esto conlleva que en la investigación deben adoptarse las medidas necesarias para que las fuentes de prueba, derivadas de la prueba digital producto de vigilancia secreta, lleguen al proceso penal en el mismo estado o las mismas condiciones en que fueron obtenidas, sin ningún tipo de alteración. Lo que permite establecer: a) que se trata de la misma fuente de prueba (autenticidad) y b) que la misma no ha sido manipulada o alterada (integridad).

Delgado Martín expresa que *la autenticidad* en el ámbito de la prueba digital consiste en garantizar la autenticidad de origen de los datos, es decir de la fuente de la que proceden los mismos. Y en cuanto a *la integridad*, la describe como la propiedad o característica consistente

[45] DE LA TORRE RODRIGUEZ, Pedro. La Prueba Digital en el Proceso Judicial. Disponible en: https://indalics.com/blog-peritaje-informatico/prueba-digital

en que los datos no han sido alterados de manera no autorizada, es la cadena de custodia o preservación de los datos[46].

Ahora bien, en lo que tiene que ver con la prueba pericial informática, la misma resulta admisible cuando: a) se requiere el acceso a la información contenida en un dispositivo, b) la información ha sido encriptada o eliminada, y c) cuando el acceso a dicha información es complejo y requiera de conocimientos técnicos o especiales. Algunas fases del dictamen pericial informático son: la obtención de los datos (acceso a la información), el clonado de los datos y cálculo del *hash,* la elaboración del dictamen y su presentación.

En el diseño de la pericia por el experto informático y en los posteriores juicios de admisibilidad y valoración de la prueba que realiza el juez, deberá tenerse en consideración la confiabilidad de la información, la cual dependerá de mecanismos técnicos que garanticen la integralidad, la inalterabilidad, la rastreabilidad, la recuperabilidad y la conservación. Al respecto, la Corte Constitucional colombiana explica estos elementos que se presentan en la Tabla 1.

Tabla N.° 1. Criterios para la admisibilidad de la prueba digital

Integralidad	Asegura que el contenido transmitido electrónicamente sea recibido en su totalidad
Inalterabilidad	Garantiza la permanencia del mensaje en su forma original, mediante sistema de protección de información
Rastreabilidad	Permite el acceso a la fuente original de la información
Recuperabilidad	Posibilita su posterior consulta
Conservación	Perdurabilidad en el tiempo contra deterioros o destrucción por virus informáticos

Fuente: Elaboración propia con base en Corte Constitucional de Colombia. Sentencia C-604 de 2016. M. P. Luis Ernesto Vargas Silva. 2 de noviembre de 2016.

[46] DELGADO MARTIN, Joaquín. ¿Cómo afrontar la complejidad de la prueba digital? Una visión práctica para los profesionales del derecho. *Derecho Digital e Innovación,* N.° 2. Madrid: Ed. Wolters Kluwer, abril-junio de 2019.

De otro lado, se destaca que en los sistemas penales de España y Colombia pueden hacerse uso del agente encubierto informático, cuya tarea es infiltrarse en una red para realizar una vigilancia secreta y examinar la información relacionada con los hechos investigados. Esta actuación está sometida al control de legalidad del juez de instrucción (España) o del juez de control de garantías (Colombia). Otros métodos de investigación criminal consisten en la interceptación de comunicaciones, la recuperación de información que circula a través de redes de comunicación (por ejemplo, las redes sociales), la búsqueda selectiva en bases de datos, la grabación directa de comunicaciones orales, la captura de imágenes, y el uso de dispositivos de seguimiento y geolocalización.

Igualmente, estos actos de indagación y de investigación autorizan a que las autoridades de policía judicial, bajo la coordinación del Ministerio Fiscal, puedan acceder a la información que reposa en dispositivos móviles, discos de almacenamiento portátil, dispositivos electrónicos e incluso que reposan en la nube. Téngase en cuenta que se puede conservar información digital a través de diferentes medios de almacenamiento como tabletas, USB, correos electrónicos y teléfonos celulares, que sirven para probar hechos relevantes en el proceso judicial. Su acceso no autorizado a información personal puede desconocer el derecho a la intimidad del titular, salvo que medie su autorización expresa o que exista una orden de autoridad judicial competente.

Todas estas intervenciones sin duda limitan o restringen derechos fundamentales como la intimidad personal, el secreto de las comunicaciones, la protección de datos personales o la autodeterminación informativa. De ahí la importancia de que en los procedimientos de indagación e investigación, se sigan las disposiciones normativas y jurisprudenciales para la obtención de las autorizaciones judiciales que exija cada sistema o el sometimiento a los controles posteriores que disponen los procesos penales. Todo ello en aras de contrarrestar el riesgo de que los medios cognoscitivos obtenidos deriven en prueba ilícita por vulneración de los derechos fundamentales y generen su evidente rechazo o exclusión, según el momento procesal de verificación de tal condición nociva.

Con todo, el juicio de admisibilidad probatoria, no es más que el resultado de un juicio que realiza el juez sobre las condiciones del medio o actividad probatorios que se proponen para su admisión en el proceso

penal. En ese sentido, deberá establecerse si se cumplen los requisitos de necesidad, pertinencia, utilidad, y legalidad.

Tabla N.° 2. Requisitos de necesidad, pertinencia, utilidad, y legalidad según las normativas española y colombiana

Criterio de admisibilidad	Característica
Necesidad	Para el caso de Colombia, no es necesario probar hechos sobre los que exista acuerdo entre las partes[47] No es necesario probar hechos notorios de manera general
Pertinencia	Existe relación en el hecho que se pretende probar mediante el medio de prueba y los hechos objeto de controversia en el proceso
Utilidad	Es inútil cuando el medio de prueba no contribuye a esclarecer los hechos o hay redundancia probatoria
Legalidad	Es ilegal cuando se pretender acreditar un hecho por medio de una actividad contraria a la ley

Fuente: Elaboración propia con base en normativas española y colombiana.

Adicionalmente, Magro Servet, magistrado del Tribunal Supremo de España, describe que para admitir la evidencia digital se deben cumplir los criterios que se presenta en la Tabla 3.[48]

Tabla N.° 3. Criterios de admisibilidad de la prueba digital

Criterio de admisibilidad	Para la prueba digital
Licitud	La obtención de la evidencia digital no puede vulnerar el derecho a la intimidad del afectado protegido constitucionalmente. Tampoco puede vulnerar el secreto de las comunicaciones. Y deberán tenerse en cuenta criterios de proporcionalidad, idoneidad, necesidad y justificación.

[47] Criterio no aplicable en la experiencia española

[48] MAGRO SERVET, Vicente. Casuística práctica de la prueba digital en el proceso civil y penal. *Actualidad Civil*, N.° 1, enero 2020.

Criterio de admisibilidad	Para la prueba digital
Integridad	Que se garantice la inmutabilidad del soporte, de manera que la muestra obtenida para realizar la evidencia electrónica quede indubitada, como base sobre la que se hará el análisis forense.
Autenticidad	Para garantizar que la muestra sobre la que se hace la investigación es idéntica a la muestra original. Ello se garantiza con la cadena de custodia, que comprende el proceso de acceso, obtención, transferencia y almacenamiento de los datos.
Claridad	Insertarse a través de informe de perito con cualificación técnica, para conocimiento y claridad del juez.

Fuente: Elaboración propia.

Por su parte, Merida y Lázaro[49], hace más de una década, reflexionaban en torno a los requisitos legales de admisión de la prueba electrónica, los cuales clasificaron en requisitos generales y requisitos técnicos. Entre los *requisitos generales*, destacan las autoras: la finalidad legal, la utilidad, el respeto de los derechos fundamentales (respeto de la privacidad y del secreto de las comunicaciones), la relevancia, la eficacia, la pertinencia, la necesidad, la proporcionalidad y razonabilidad, la transparencia durante la obtención, y la facilitación de los medios de exhibición. Y en cuanto a los *requisitos técnicos*, enuncian los siguientes: identificación del remitente, garantía de integridad, almacenamiento en condiciones de seguridad, confidencialidad, requisitos de verificación de envío y entrega, seguridad de la prueba, información previa al propietario del ordenador y requisitos técnicos del certificado electrónico.

Con relación a la valoración, téngase en cuenta que, tanto en el sistema procesal penal español como en el colombiano, se configura la libre valoración probatoria sustentada en las reglas de la sana crítica. Y es la senda en la que, el juez deberá analizar si existe prueba de cargo

[49] MERIDA, Fredesvinda Insa; LÁZARO, Carmen. La admisibilidad de las pruebas electrónicas en los tribunales (A.P.E.T): Luchando contra los delitos tecnológicos. *La Ley,*. Madrid: Ed. Wolters Kluwer, 2007

sometida a los principios de inmediación, contradicción, publicidad e igualdad; realizar un juicio de suficiencia, que de existir prueba de cargo deberá comprobar si la misma es suficiente para desvirtuar la presunción de inocencia, y además deberá motivar razonadamente si la presunción de inocencia se ha desvirtuado.

Frente a la prueba o evidencia digital, esta debe cumplir con los *requisitos intrínsecos* de autenticidad, integralidad, fiabilidad y disponibilidad, así como con los *requisitos extrínsecos* de legalidad (obtenida y practicada con el cumplimiento de los requisitos legales) y de licitud (obtenida y practicada sin el desconocimiento de derechos fundamentales) para ser valorada en el proceso. Asimismo, la valoración de la evidencia digital se lleva a cabo a partir de la apreciación conjunta, pudiendo el juez restarles valor probatorio a chats, fotografías, videos, correos electrónicos, etc., que llegaren a ser alterados o modificados por la mano de las partes o de terceros.

De acuerdo con Delgado Martín, la libre valoración de la prueba digital se representa en los siguientes aspectos[50] que se sintetizan así:

1. La ley no obliga al juez a tener por probados los hechos que surjan de una prueba digital.
2. La prueba digital puede tener efectos para acreditar un hecho relevante para el proceso.
3. La eficacia probatoria que el juez otorga a la prueba digital, está sujeta a la aplicación de las reglas de la sana crítica.
4. El componente tecnológico de la prueba digital determina la importancia de los conocimientos científicos en su valoración, es allí donde la prueba pericial informática tiene mayor importancia.
5. La prueba digital debe ser valorada en relación con los demás medios de prueba.

Ahora bien, cuando en la práctica de la prueba digital se deben adoptar medidas como la intervención de las comunicaciones telefónicas o telemáticas, si las mismas se practican con vulneración de un derecho

[50] DELGADO MARTÍN, Joaquín. Op. cit. 2017; DELGADO MARTÍN, Joaquín. Op. cit. 2019.

fundamental, el juez no puede conferirle valor probatorio, y por tratarse de una prueba ilícita no tendrá validez ni podrá destruir la presunción de inocencia[51].

3.2 Precisiones sobre admisibilidad y valoración de la prueba digital producto de la vigilancia secreta en la experiencia de investigación penal en España

En el proceso penal de adultos, quien dirige la investigación en España es el juez de instrucción. El Ministerio Fiscal será parte activa en los procesos perseguibles de oficio. Sin embargo, en el procedimiento por delitos menos graves (llamado "procedimiento abreviado", aunque no depende de que haya conformidad alguna, sino solo de que estemos ante el ámbito objetivo de delitos cuya pena privativa de libertad no sea superior a nueve años o se trate de penas de otra naturaleza, y que no corresponda a ningún otro procedimiento, como el de enjuiciamiento rápido, el del Tribunal del Jurado, o el de delitos leves), se prevé una posibilidad de investigación preliminar por los fiscales en el art. 773.2 de la LECrim[52].

---

[51] ÁGUILA SÁNCHEZ, Cristina. La interceptación de las comunicaciones telefónicas y telemáticas en el proceso penal. *Diario La Ley,* N.° 9303. Madrid: Ed. Wolters Kluwer, 21 de noviembre de 2018.

[52] "Cuando el Ministerio Fiscal tenga noticia de un hecho aparentemente delictivo, bien directamente o por serle presentada una denuncia o atestado, informará a la víctima de los derechos recogidos en la legislación vigente; efectuará la evaluación y resolución provisionales de las necesidades de la víctima de conformidad con lo dispuesto en la legislación vigente y practicará él mismo u ordenará a la Policía Judicial que practique las diligencias que estime pertinentes para la comprobación del hecho o de la responsabilidad de los partícipes en el mismo. El Fiscal decretará el archivo de las actuaciones cuando el hecho no revista los caracteres de delito, comunicándolo con expresión de esta circunstancia a quien hubiere alegado ser perjudicado u ofendido, a fin de que pueda reiterar su denuncia ante el Juez de Instrucción. En otro caso instará del Juez de Instrucción la incoación del procedimiento que corresponda con remisión de lo actuado, poniendo a su disposición al detenido, si lo hubiere, y los efectos del delito. El Ministerio Fiscal podrá hacer comparecer ante sí a cualquier persona en los términos establecidos en la ley para la citación judicial, a fin de recibirle declaración, en la cual se observarán las mismas garantías señaladas en esta Ley para la prestada

3.2.1. Sobre la admisibilidad y valoración de los resultados de la investigación

La investigación que estamos analizando no tiene sólo el propósito de averiguar los datos que puedan ser útiles para formular la acusación en el momento procedimentalmente previsto -y, en su caso, también para la defensa-, sino además por las propias características de los hechos investigados deberán constituirse con frecuencia pruebas preconstituidas, pues de manera constante estaremos ante diligencias investigadoras de naturaleza irrepetible[53]. En todo caso el acervo probatorio obtenido habrá de ser sometido a los principios constitucionales de audiencia y contradicción en la fase plenaria que eventualmente pueda celebrarse.

Por otro lado, en el ordenamiento español, tenemos el problema de que los avances conseguidos con la promulgación de las citadas reformas legislativas, que ofrecen un amplio abanico de novedosas diligencias de investigación que consisten en la aplicación de tecnologías digitales, no se corresponden con una actualización respecto al cauce de entrada al juicio oral como medios de prueba. En definitiva, hay un desfase entre el reconocimiento de nuevas fuentes de prueba y el mantenimiento de la regulación antigua por lo que se refiere a los medios de prueba. Ello contrasta con lo ocurrido en el orden jurisdiccional civil, pues el código procesal civil promulgado por la Ley 1/2000, de 7 de enero – llamado en España, Ley de Enjuiciamiento Civil- incluyó expresamente entre los medios de prueba la prueba informática y la prueba videográfica, aunque de una manera más periférica ("los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso" art. 299.2 y en los arts. 382 a 384). Por lo tanto, se plantea la

ante el Juez o Tribunal. Cesará el Fiscal en sus diligencias tan pronto como tenga conocimiento de la existencia de un procedimiento judicial sobre los mismos hechos".

53 DURÁN SILVA, Carmen. Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado. Revista la Ley *Penal,* N.° 126 . Madrid: Ed. Wolters Kluwer, 2017.

pregunta de cómo incorporar al juicio oral los resultados obtenidos a través de los medios tecnológicos novedosos.

Una de las soluciones interpretativas que prodría intentarse es aplicar la regla de aplicación supletoria de la LEC (art. 4), por la que en defecto de disposiciones que regulan los procesos penales, serán de aplicación los preceptos de esta ley. Otra vía interpretativa podría ser la aplicación de la Ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y las comunicaciones en la Administración de Justicia, y la disposición adicional primera de la Ley 42/2015, de 5 de octubre, que regula la utilización de los medios telemáticos para la presentación de "escritos y documentos". Por su parte, en la Ley 59/2003, de 19 de diciembre, de firma electrónica, encontramos una definición sobre "documento electrónico" qu podría ser útil a los efectos que estamos considerando: "Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado" (art. 3.5). Debemos tener en cuenta, sin embargo, que esta última Ley fue derogada por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, que a su vez contiene en su artículo 3 l una mención mucho más genérica ("Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable").

Todas las soluciones que acabamos de considerar podrían suscitar argumentos en su favor, sin embargo, en el ámbito penal, la jurisprudencia[54] sigue aprovechando las ventajas de una regulación

[54] Como afirma, por todas, la sentencia de la Sala 2.ª, de lo Penal, de 26 de septiembre de 2000, del Tribunal Supremo español: "Las grabaciones videográficas, constituyen incuestionablemente un documento, que puede ser esgrimido a los efectos de sustentar un posible error de hecho en la apreciación de la prueba. De conformidad con lo dispuesto en el art. 26 del Código Penal, constituye un soporte gráfico que incorpora hechos, impresionados en cinta incorporada a la cámara que grabó las incidencias del suceso que se imputa al recurrente. Una reiterada jurisprudencia de esta Sala las equipara, en su consideración de documento, no solo a los escritos tradicionales, sino también a cualquier otra representación gráfica del pensamiento o de la realidad, que, a

amplia y suficientemente indeterminada del concepto de "documento". En efecto, no la LECrim, sino el Código Penal es el que nos suministra una definición omnicomprensiva, al disponer su art.26 que es "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica". Así, el acervo probatorio obtenido a través de los medios de investigación a los que nos hemos referido en las páginas anteriores, con fotografías, imágenes videográficas, esquemas cartográficos o termografías, entre muchas otras posibilidades ingresan a la fase plenaria del proceso penal español como simples documentos. Pero esta posición jurisprudencial no es irrelevante, pues puede conllevar algunas cuestiones problemáticas. En principio, simplemente será necesario presentar el documento junto al correspondiente escrito de acusación o de calificaciones provisionales y en fase de instrucción. En el supuesto de la prueba documental, no hay necesidad alguna de que el sujeto que ha obtenido tales datos digitales deba someterse a interrogatorio en el debate oral. Pero puede haber discusiones sobre cómo se ha podido adquirir tal "documento" o cómo ha podido asegurarse su conservación sin alteraciones. Sin poder preguntar sobre ello a la persona responsable de su obtención, parece que quedaría limitado el debate contradictorio, pudiendo resultar indefensiones claras. Como es fácil de deducir, cuando estamos tratando de medios cuyo manejo exige una indispensable especialización, sería recomendable una asimilación a la prueba pericial, de modo que el que ha obtenido los datos a través de la vigilancia secreta, sea sometido a un interrogatorio cruzado respecto a los pormenores que las partes procesales tengan a bien preguntar, siempre que, obviamente, el tribunal las considere pertinentes y necesarias.

De este modo puede propiciarse un mejor ejercicio del derecho de defensa y una más plena aplicación del principio de contradicción. La mejor opción, en nuestra opinión, sería la previsión expresa de un

través de su examen o visionado, se pueda conocer o comprobar". Aplicando esta doctrina jurisprudencial, véanse, entre muchas otras, las sentencias de la Audiencia Provincial de Barcelona, Audiencia Provincial de Barcelona, Sección 9ª, de 24 de julio de 2019, o la de Audiencia Provincial de Guadalajara, Sección 1ª, de 19 de noviembre de 2020.

medio de prueba autónomo[55], como prueba digital[56] para la que no sea suficiente la presentación de los datos destinados al juicio oral, sino sobre todo su explicación detallada, las cuestiones relativas al modo de adquisición, las inferencias que de ellos pueden obtenerse, en definitiva, colocarlos al nivel de plena comprensión para las partes y para el órgano jurisdiccional[57]. Con este nuevo medio de prueba, además, evitaríamos alargar más la duración del proceso, pues si partimos de considerarlos prueba documental, posiblemente sea necesaria una solicitud adicional de prueba, a fin de discutir algunos elementos de los documentos presentados, por tanto, podría ser imprescindible, la admisión de pericias que puedan aclarar las dudas que se susciten, o que permitan una mayor comprensión y apreciación de la prueba a los profanos, entre los que se encuentra muy probablemente el juzgador mismo.

Por supuesto, la labor de apreciación y de valoración de los resultados probatorios implica riesgos. El órgano jurisdiccional debe construir narrativamente la relación de hechos probados a partir de lo practicado y discutido en el juicio oral. En los casos que estamos analizando probablemente el riesgo principal sea el de la tentación de confundir lo obtenido en la vigilancia secreta con la realidad de los hechos. Somos conscientes de que esta afirmación precisa de una mayor explicación. Nos referimos a que al hacer ingresar en el proceso imágenes, videograbaciones, o incluso datos, puede parecer que traemos

---

[55] Sobre las dificultades terminológicas de estas pruebas, *véase* DÍAZ LIMÓN, Jaime Alberto. Incorporación de la prueba cibernética e informática: electrónica y digital, *Revista del Instituto Colombiano de de Derecho Procesal,* N.° 47. Bogotá: Ed. Instituto Colombiano de Derecho Procesal, 2018.

[56] CARRIER, Brian.; SPAFFORD, Eugene. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, vol. 2, 2003, ofrecían ya una definición de tal medio de prueba, como el que permite obtener datos digitales, es decir, "that can establish that a crime has been committed, can provide a link between a crime and its victim, or can provide a link between a crime and its perpetrator. The data in memory, on the hard disk, or in a cell phone are examples of digital evidence". *Véase* asimismo, DE AGUILAR GUALDA, Salud. *La Prueba Digital en el Proceso Judicial: Ámbito Civil y Penal*, primera edición, Barcelona, 2019, pp. 111–130.

[57] *Véase* más ampliamente, GARRIE, Daniel; MORRISSY, David. Digital Forensic Evidence in the Courtroom: Understanding Content and Quality. *Northwestern Journal of Technology and Intellectual Property*, vol. 12, N.° 2, 2014.

al juicio la realidad misma. Confundiríamos así el medio de prueba con la realidad histórica que necesita ser probada. Así pues, al parecer que así sabemos directamente qué ocurrió y dónde -incluso lo estamos viendo-, para el juzgador puede ser un elemento probatorio fundamental e indiscutible. Los psicólogos jurídicos, no obstante, nos avisan de que la verosimilitud de lo que se muestra no nos debe llevar a la conclusión errónea de que traemos al proceso la realidad misma[58]. Lo que se trae es una representación de la realidad, más o menos fiel, pero que puede ser parcial, por tanto, que no tenga en cuenta todos los elementos de la realidad, porque algunos se quedan fuera inevitablemente de la prueba digital presentado en juicio, sí basáramos la convicción sobre los hechos punibles en esa visión limitada, en realidad fundamentaríamos la narración de hechos probados en una cognición eventualmente parcial. Como en todos los casos, es preciso asegurar la cadena de custodia, de modo que lo obtenido con estos medios de investigación no supongan una alteración de la fuente de prueba, pero además, es preciso que en la valoración se tenga el cuidado suficiente para ser consciente del efecto de enmarcamiento que producen este tipo de pruebas, sobre todo las de carácter videográfico, pero no solo ellas. Tampoco podemos olvidar que existe otro riesgo respecto a la valoración de estas pruebas tecnológicas: el posible efecto de embelesamiento acrítico que puede llevar a aceptar sin apenas discusión lo que procede de medios relacionados con tecnologías digitales[59]. No se nos entienda mal, no pretendemos restringir la utilización de este tipo de pruebas, sino básicamente hacer consciente al juzgador de la labilidad que también puede caracterizar estas pruebas, para que no se engañe a fin de obtener genuinamente la simple verdad de lo que se trata de enjuiciar[60].

---

[58] Cfr. FEIGENSON, Neal. *Law on Display: The Digital Transformation of Legal Persuasion and Judgment*. New York: New York University Press, 2009.

[59] BUJOSA VADELL, Lorenzo Mateo. Tecnologías ambientales y delitos ambientales, *Revista Eletrônica de Direito Processual,* vol. 20, N.° 3. Rio de Janeiro: vLex, 2019, pp. 268-292.

[60] Cfr. TARUFFO, Michele. *Simplemente la verdad: El juez y la construcción de los hechos.* Madrid: Marcial Pons, 2010.

Conclusiones

El tránsito desmesurado a la interacción digital ha propiciado el surgimiento de nuevas modalidades delictivas en lo que hoy se identifica como cibercrimen. Por ello, el derecho penal en el aspecto sustancial, procesal y probatorio debe adaptarse a esta realidad global, sin perder de vista el equilibrio necesario entre el derecho a la verdad, la justicia y la reparación de las víctimas y los derechos y garantías procesales que limitan el actuar investigativo en favor del imputado y/o acusado. De ahí que se debe fortalecer el poder punitivo con investigaciones y mecanismos digitales.

La prueba digital atraviesa por las fases de obtención de la información o datos, la incorporación de los datos al proceso y la valoración de los datos incorporados. En la práctica se observa que con mayor frecuencia se incautan equipos informáticos o dispositivos de almacenamiento de datos, y se registra la vigilancia secreta a través de estos medios. Al respecto, resulta importante su contenido para el proceso penal a través del reconocimiento del propio investigado, la declaración de los testigos, que incluye a los investigadores de campo y los peritos informáticos como testigos de acreditación, como también es relevante la pericia informática acompañada de la declaración como testigo experto del perito informático.

Todo ello conduce a pensar en los elementos que integran la prueba digital: desde la fuente de prueba (su autenticidad), que la misma no haya sido manipulada o alterada (su integridad), la garantía de permanencia del mensaje en su forma original (inalterabilidad), el acceso a la fuente original de información (rastreabilidad), la posibilidad de posterior consulta (recuperabilidad) y, en especial, la perdurabilidad en el tiempo (su conservación).

De esta manera, se destacan como criterios de admisibilidad de la prueba digital, producto de la vigilancia secreta: la licitud, la integridad, la autenticidad y la claridad. Asimismo, para su valoración probatoria se han delimitado, con base en la doctrina, una serie de requisitos intrínsecos (autenticidad, integridad, fiabilidad y disponibilidad) sumados a unos requisitos extrínsecos de legalidad y licitud.

Para la validez y eficacia de la vigilancia secreta, es recomendable la adecuación del sistema normativo en cada país, encontrar la coherencia

de la gestión investigativa con el orden convencional consolidado para la protección humana, documentar la delimitación operacional, determinar y ejecutar una capacitación especial para los órganos de investigación y control judicial. Además, se debe precisar la interacción requerida entre los desarrollos tecnológicos y los protocolos de procedimiento en la gestión penal contra el crimen, en especial contra el cibercrimen.

La obtención de material probatorio a través de medios de vigilancia secreta plantea serios riesgos que multiplican su complejidad cuando aplicamos instrumentos o dispositivos digitales o electrónicos. Nos permite aumentar las posibilidades de la investigación penal, pero también es mayor la exposición de los derechos fundamentales ante la expansión de las vías de pesquisa.

Para contar con idoneidad fáctica y jurídica, las tecnologías utilizadas para la vigilancia secreta en el ámbito de la persecución criminal, deben contar con estándares de desarrollo estructural según su programación inteligente y niveles de medición que sean controlados por comités profesionales integrados interdisciplinariamente, y así garantizar su operación y ajuste oportuno, de acuerdo con el acervo de garantías definidas y acordadas nacional e internacionalmente.

Las novedades que observamos en ordenamientos como el español nos parecen un paso adelante con el fin de encauzar las debidas prevenciones ante esas actuaciones del poder público. Establecer en las normas procesales penales los criterios concretos para la aplicación de esas medidas restrictivas de derechos es una manera loable de ajustar la investigación a las exigencias convencionales y constitucionales. Sin embargo, hay que evitar aún algunas referencias a conceptos indeterminados como "la trascendencia social" de los hechos investigados, pues introducen inadecuados elementos de eventual arbitrariedad.

En todo caso, la innovación debiera ser completa y actualizar también los cauces a través de los cuales ese material probatorio puede entrar en la fase plenaria del proceso, y ofrecer además criterios de ponderación en la autorización previa de actuación judicial y de valoración de la prueba practicada que no confundan la realidad que se pretende enjuiciar con lo que es una representación de la misma, la cual debe servir para la construcción narrativa que deberá expresarse con claridad en la motivación de la sentencia.

REFERENCIAS

ABEL LLUCH, X.; RICHARD GONZÁLEZ, M. *Estudios sobre la Prueba Penal*. Madrid: Editorial La Ley. 2013.

ACEVEDO SURMAY, D.; GÓMEZ USTARIS, É. Los documentos electrónicos y su valor probatorio en procesos de carácter judicial. *Iustita. Revista de la División de Ciencias Jurídicas y Políticas*, n. 9, p. 391–419. 2011. https://doi.org/10.15332/iust.v0i9.905

ÁGUILA SÁNCHEZ, C. La interceptación de las comunicaciones telefónicas y telemáticas en el proceso penal. *Diario La Ley*, n. 9303, Sección Tribuna, Ed. Wolters Kluwer. 2018. https://dialnet.unirioja.es/servlet/articulo?codigo=6667260

AGUILERA MORALES, M. *Proceso penal y causa general en el Derecho español*. Madrid: Aranzadi-Civitas-Thomson Reuters. 2008.

ARMENTA DEU, T. Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre. *Revista de Internet, Derecho y Política,* n. 27. 2018. https://doi.org/10.7238/idp.v0i27.3149

ARRABAL PLATERO, P. *Tratamiento procesal de la prueba tecnológica*. Tesis (Doctorado en Ciencias Sociales y Jurídicas). Madrid: Universidad Miguel Hernández, 2019.

ASENCIO MELLADO, J. M. La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita. *Diario La Ley,* n. 9499. 2019. https://diariolaley.laleynext.es/dll/2019/10/16/la-stc-97-2019-de-16-de-julio-descanse-en-paz-la-prueba-ilicita

BARREIRA, M. V. Impacto de las nuevas tecnologías en la prueba judicial civil. *Revista de Derecho de la Universidad de Montevideo*, n. 37, p. 139-176. 2020. https://doi.org/10.47274/DERUM/37.7

BUENO DE MATA, F. *Las diligencias de investigación en la cuarta revolución industrial. Principios teóricos y problemas prácticos*. Madrid: Aranzadi, Cizur Menor. 2019.

BUJOSA VADELL, L. M., Tecnologías ambientales y delitos ambientales, *Revista Eletrônica de Direito Processual,* vol. 20, n. 3, p. 268-292. 2019. http://doi.org/10.12957/redp.2010.45021

CAMPOLI, G. A. *Manual Básico de Cateo y Aseguramiento de Evidencia Digital*. Bogotá: vLex International, n. 14, mayo. 2013.

CARRIER, B.; SPAFFORD, E. H. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, vol. 2, n. 2, Fall. 2003. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf

CRUZ TEJADA, H. *La prueba documental electrónica frente al documento en soporte papel*. Nuevas tendencias del derecho probatorio. Bogotá: Ediciones Uniandes, segunda edición. 2015.

DE AGUILAR GUALDA, S. *La Prueba Digital En El Proceso Judicial: Ámbito Civil y Penal*, 1a edición, Barcelona, p. 111–130. 2019. https://doi.org/10.2307/j.ctvwcjgj0.7

DELGADO, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: La Ley. 2016.

DELGADO, J. La valoración de la prueba digital. *Diario La Ley,* n. 6, Sección Ciberderecho, Ed. Wolters Kluwer. 2017.

DELGADO, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª edición, Madrid: Ed. Wolters Kluwer. 2018.

DELGADO, J. ¿Cómo afrontar la complejidad de la prueba digital? Una visión práctica para los profesionales del derecho. *Derecho Digital e Innovación,* n. 2, abril-junio. 2019, Ed. Wolters Kluwer.

DE LA TORRE RODRÍGUEZ, P. *La Prueba Digital en el Proceso Judicial*. https://indalics.com/blog-peritaje-informatico/prueba-digital

DÍAZ LIMÓN, J. Incorporación de la prueba cibernética e informática: electrónica y digital. *Revista del Instituto Colombiano de Derecho Procesal,* n. 47, p. 19-42. 2018. http://dx.doi.org/10.32853/01232479.v47.n47.2018.475

DURÁN SILVA, C. Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado. *La Ley Penal*, n. 126, mayo-junio. 2017.

ESCALANTE BARRETO, E. *El agente encubierto informático como Técnica Especial de Investigación en la lucha contra el crimen organizado*. Bogotá: vLex International, n. 48, julio. 2019.

FEIGENSON, N.; CORCOS, C. A.; SPIESEL, C. *Law on Display: The Digital Transformation of Legal Persuasion and Judgment*. New York: New York University Press. 2009. https://doi.org/10.1007/s11196-010-9169-6

GARRIE, D. B.; MORRISSY, J., D. Digital Forensic Evidence in the Courtroom: Understanding Content and Quality. *Northwestern Journal of Technology and Intellectual Property*, vol. 12, n. 2. 2014.

LOPEZ BARAJAS PEREA, I. Garantías Constitucionales en la Investigación Tecnológica del delito: previsión legal y calidad de la Ley. *Revista de Derecho Político*, Madrid, n. 98, enero-abril, p. 91-119. 2017. https://doi.org/10.5944/rdp.98.2017.18652

MAGRO SERVET, V. Casuística práctica de la prueba digital en el proceso civil y penal. *Actualidad Civil,* n. 1, enero. 2020. Ed. Wolters Kluwer.

MERIDA, F. I.; LÁZARO, C. La admisibilidad de las pruebas electrónicas en los tribunales (A.P.E.T): Luchando contra los delitos tecnológicos. *La Ley,*. Madrid: Ed. Wolters Kluwer. 2007

MOENSSENS, A.; DESPORTES, B.; EDWARDS, C. *Scientific Evidence in Civil and Criminal Cases*. New York: Foundation Press. 2013.

NARANJO GÓMEZ, B.; MENDOZA PÉREZ, J.; ALONSO BETANCOURT, E.; HINOJOZA CALZADA, J. Informática criminalística: una especialidad en desarrollo. *Opinión Jurídica,* vol. 19, n. 38, p. 245-257, ene-jun. 2020. https://doi.org/10.22395/ojum.v19n38a12

RODRÍGUEZ ÁLVAREZ, A. Intervención de las comunicaciones telefónicas y telemáticas y *smartphones*. Un primer estudio a propósito de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal. En: ASENCIO MELLADO, J. M. (Dir.). *Justicia penal y nuevas formas de delincuencia*. Valencia: Tirant lo Blanch. 2017.

RODRÍGUEZ LAINZ, J. La nueva jurisprudencia sobre dispositivos de seguimiento y localización (Comentario a la STS, Sala 2ª, 141/2020, de 13 de mayo). *Diario La Ley*, n. 9650, junio. 2020.

SALAMANCA AGUADO, E. El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones. *Revista del Instituto Español de Estudios Estratégicos (IEEE),* n. 4. 2014. https://revista.ieee.es/article/view/306

TARUFFO, M. *Simplemente la verdad: El juez y la construcción de los hechos*. Madrid: Marcial Pons. 2010.

TORO GARZÓN, L.; BUSTAMANTE RÚA, M. La investigación y la prueba de contexto como elementos de política criminal para la persecución del crimen organizado. *Revista Criminalidad*, vol. 62, n. 1, p. 101-115, enero-abril. 2020. http://www.scielo.org.co/pdf/crim/v62n1/1794-3108-crim-62-01-00101.pdf

VELASCO NÚÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*. Madrid: Sepin. 2016.

VIOLLIER BONVIN, P.; ORTEGA ROMO, V. Cuando el Estado Hackea: El caso de operación Huracán. *Revista Chilena de Derecho y Tecnología,* v. 8, n. 2, p. 83-110. 2019. https://doi.org/10.5354/0719-2584.2019.54436

Additional information and author's declarations
(scientific integrity)

Acknowledgement: We thank the Universidad de Medellín and the Universidad de Salamanca for their support in carrying out this research.

Conflict of interest declaration: the authors confirm that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

- *Lorenzo Mateo Bujosa Vadell*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.
- *Mónica María Bustamante Rúa*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.
- *Luis Orlando Toro Garzón*: conceptualization, methodology, data curation, investigation, writing – original draft, validation, writing – review and editing, final version approval.

Declaration of originality: the authors assure that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; they also attest that there is no third party plagiarism or self-plagiarism.

Editorial process dates
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Submission: 15/12/2020
- Desk review and plagiarism check: 08/01/2021
- Ressubmission and transferente to V7N3: 23/02/2021
- Review 1: 06/03/2021
- Review 2: 08/03/2021
- Review 3: 06/03/2021
- Preliminary editorial decision: 16/05/2021
- Correction round return: 21/06/2021
- Final editorial decision: 25/06/2021

Editorial team
- Editor-in-chief: 1 (VGV)
- Reviewers: 3

HOW TO CITE (ABNT BRAZIL):

BUJOSA VADELL, Lorenzo M.; BUSTAMANTE RÚA, Mónica M.; TORO GARZÓN, Luis O. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, vol. 7, n. 2, p. 1347-1384, mai./ago. 2021. https://doi.org/10.22197/rbdpp.v7i2.482