Foro, Nueva época, vol. 23, núm. 1 (2020): 267-304 ISSN: 1698-5583
https://dx.doi.org/10.5209/foro.74004

NUEVAS DILIGENCIAS DE INVESTIGACIÓN Y DE PRUEBA: EL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

Carmen Rodríguez Rubio
Profesora de Derecho Procesal
Departamento de Derecho Público II y Filología I
Facultad de Ciencias Jurídicas y Sociales
Universidad Rey Juan Carlos
mariacarmen.rodriguez@urjc.es

I. INTRODUCCIÓN

Desde hace tiempo se pretende la elaboración de una nueva ley procesal, siendo diversas las manifestaciones que se han hecho en esta dirección. Así, en su momento, el Pacto de Estado para la Reforma de la Justicia de 28 de mayo de 2001 estableció diversos objetivos entre los cuales se anunciaba la redacción de una nueva Ley de Enjuiciamiento Criminal; una ley procesal en la que, entre otras cosas, se lograra la regulación de métodos de investigación para delitos de nuevo cuño y en la que los medios de prueba se adaptaran a los últimos avances tecnológicos. Tras el Pacto de Estado para la Reforma de la Justicia ha habido diversas propuestas: en primer lugar se deben mencionar los Anteproyectos de Ley para un Nuevo Proceso Penal (2011), distinguiéndose, por un lado, el Anteproyecto de Ley Orgánica de Desarrollo de los Derechos Fundamentales vinculados al Proceso Penal y, por otro, el Anteproyecto de Ley de Enjuiciamiento Criminal[1]. Estos documentos se caracterizan, principalmente, por ser textos articulados, esto es, propuestas que avanzan a través de numerosos preceptos cómo se sustanciará el proceso en el futuro. Por otra parte, también se ha de tener presente la Propuesta de texto articulado de Ley de Enjuiciamiento Criminal, elaborada por la Comisión

[1] Ministerio de Justicia, Secretaría General Técnica, NIPO: 051-11-029-4, DL: M-32828-2011.

Institucional creada por acuerdo del Consejo de Ministros de 2 de marzo de 2012[2], en cuya exposición de motivos se pone de manifiesto de manera clara cómo es necesario abordar una regulación detallada de las nuevas diligencias de investigación y de otros actos propios de la fase de instrucción ya utilizados en el proceso, pero que necesariamente requieren ser actualizados.

También siguiendo esta línea de pretendidas reformas, que se hace tan necesaria para lograr la unidad, la claridad y precisión de la ley procesal, así como cumplir con los principios de legalidad y seguridad jurídica garantizados constitucionalmente [art. 9.3 de la Constitución española (en adelante, CE)], la anterior ministra de Justicia, mediante Orden de 5 de marzo de 2019, encargó a la Sección Quinta de Derecho Procesal de la Comisión General de Codificación la elaboración de una propuesta de nueva Ley de Enjuiciamiento Criminal[3]. En dicha Orden se ponían de relieve diferentes aspectos que resultaban sustanciales en la redacción de la nueva ley. De esta manera, el nuevo texto legal recogerá un nuevo modelo en el que el Ministerio Fiscal (en adelante, MF) dirigirá la investigación y además esta estará orientada a decidir sobre el ejercicio de la acción penal. Esta idea se fundamenta en las leyes procesales de Alemania, Portugal e Italia, países inspiradores de nuestro sistema procesal y que optaron hace décadas por este modelo procesal. Dicho marco legal también ha sido seguido por casi todos los países latinoamericanos. Se trataría, por tanto, de un modelo cercano, salvando las diferencias que puedan existir, al que tiene lugar ante la Corte Penal Internacional, en el que el fiscal lleva a cabo la investigación y además es quien, en su caso, ejercita la acusación.

A esta circunstancia hay que sumar, de conformidad con la Orden, «la grave problemática de la criminalidad transfronteriza»; también la incorporación en el año 2020 de la Fiscalía Europea debido al Reglamento (UE) 2017/1939, y la existencia de equipos conjuntos de investigación penal. Continuando con lo mantenido en el mandato ministerial, en este se explica cómo al haberse regulado hace décadas en la Ley del Menor la instrucción por parte del MF y al atribuirse al Juzgado de Menores las competencias relacionadas con los derechos fundamentales, así como las funciones de enjuiciamiento y de ejecución, a lo que habrá que añadir en un futuro cercano la investigación del fiscal europeo en los delitos de los que haya

[2] Ministerio de Justicia, 2013, Secretaría General Técnica, NIPO: 051-13-010-2, Subdirección General de Documentación y Publicaciones.

[3] *www.mjusticia.gob.es* (consultado el 7 de agosto de 2019).

de conocer, existirán dos tipos de procesos, a saber: el primero, donde la fase de investigación estará atribuida al Ministerio público, y el segundo, el modelo tradicional acogido en la Ley de Enjuiciamiento Criminal en el que el juez de instrucción dirige la investigación.

De acuerdo con la Orden, todas estas circunstancias hacen necesaria la unificación del proceso, donde el MF dirija la investigación y se atribuyan al juez las funciones de garantía, enjuiciamiento y ejecución. Finalmente, la Orden establece cuáles serán los cimientos sobre los que la nueva ley se redacte: nuestras instituciones y los recientes proyectos integrales de reforma, especialmente el del año 2011, este último basado en los principios constitucionales interpretados de acuerdo con lo mantenido por el Tribunal Constitucional (en adelante, TC) y el Tribunal Europeo de Derechos Humanos (en adelante, TEDH); asimismo, solo tomará del Derecho comparado aquello sobre lo que no haya duda de que puede funcionar en nuestro país, teniendo en cuenta que el fiscal será quien dirija la investigación y que el juez tendrá las funciones anteriormente descritas y, de igual modo, se deberá integrar el jurado y tener presentes los principios de oralidad y contradicción, así como la simplificación procedimental.

Tras la Orden anterior, el actual ministro de Justicia, Juan Carlos Campo, ha anunciado recientemente la conclusión del anteproyecto de la futura Ley de Enjuiciamiento Criminal. Dicho código se ha redactado tomando en consideración los textos mencionados previamente y que empezaron su andadura con el Anteproyecto de Ley de Enjuiciamiento Criminal de 2011. Además de estos textos normativos también han servido de fundamento para su redacción dos leyes que han dado lugar a las reformas más relevantes que se han operado en la ley procesal en los últimos tiempos, a saber: Ley 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, y Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales. En el anteproyecto anunciado se dispone, entre otras cosas, la atribución de la instrucción a la fiscalía, mientras que los jueces de instrucción pasarán a ser jueces de garantías, siendo estos los que autoricen las entradas y los registros, las intervenciones telefónicas y de otro tipo y, en definitiva, todas aquellas que afecten a derechos fundamentales[4].

[4] *Confilegal.com* (consultado el 1 de octubre de 2020).

Después de lo expuesto en líneas anteriores se pueden conocer cuáles son las razones que, desde un punto de vista político-jurídico, están presentes en la elaboración de una nueva ley procesal, incluso si se profundiza en los textos que se han mencionado, estos motivos se podrán conocer con mayor amplitud. Jurídicamente, en el momento presente se dan distintas circunstancias que requieren la promulgación de una nueva ley procesal; quizá uno de los motivos que mayor peso tenga es la existencia de un texto decimonónico que ha perdido su unidad debido a las numerosas reformas que se han introducido y que están justificadas sobre todo debido al transcurso del tiempo y a los cambios que experimenta la sociedad.

En relación con los antecedentes de la ley procesal hay que tener presente, siguiendo lo mantenido por Gómez Orbaneja[5], que la Ley de Enjuiciamiento Criminal vigente se promulgó mediante Real Decreto de 14 de septiembre de 1882, procediéndose, a través del mencionado decreto, a aprobar el proyecto redactado con arreglo a la autorización concedida al Gobierno por Ley de 11 de febrero de 1881 (Ley de Bases). Como apunta el autor citado, la Ley de Enjuiciamiento Criminal marca el término de una evolución legislativa que va desarrollándose durante el siglo XIX, con alternativas y retrocesos, y que comienza con la Constitución de 1812. Lo más relevante de esta evolución es el paso de un proceso penal inquisitivo al acusatorio formal, siguiendo el modelo francés; modelo recibido en esa época en la mayor parte de las legislaciones europeas continentales. También en este sentido se pronuncia Fernández Ladreda[6] al defender que la Ley de Enjuiciamiento Criminal permitió pasar del sistema inquisitivo al acusatorio; también este autor pone de manifiesto cómo en el siglo XIX se advierte el deseo de codificar de forma separada cada rama del Derecho, siendo así como aparecen los códigos procesales.

La ley procesal vigente responde a lo que en época decimonónica se entendía por código y que Reus y Bahamonde define como «un conjunto de disposiciones que encierra todo un sistema de legislación sobre una materia determinada»[7]. El código procesal así descrito tendría dos características: la primera alude a su contenido, debido a que se extiende a una

---

[5] E. Gómez Orbaneja y V. Hercé Quemada, *Derecho Procesal Penal,* 3.ª ed., Madrid, JJP, 1951, p. 20.

[6] M. Fernández Ladreda, *Estudios históricos sobre los Códigos de Castilla,* La Coruña, Imp. y lib. de E. Carré, 1896, p. 27, disponible en *https://bibliotecadigital.jcyl.es/*.

[7] E. Reus y Bahamonde, *Ley de Enjuiciamiento Criminal de 14 de septiembre de 1882,* Madrid, Real Academia de Jurisprudencia y Legislación, 1883, p. 1, disponible en Biblioteca virtual del patrimonio bibliográfico *http://bvpb,mcu.es/*.

parcela más o menos amplia, pero total, del Derecho, y la segunda se refiere a un principio de unidad que es el que ha estado presente en su redacción. Precisamente al principio de unidad se refiere Domingo de Morato al exponer que en la España del siglo XIX hay un retorno «al apetecido estado de unidad»; en palabras del autor, existen ciertos hechos en la historia de la legislación española de importancia capital, entre ellos los sucesos políticos que se desarrollaron en el citado siglo y que dieron lugar a la unidad en el Derecho. De esta manera, Domingo de Morato divide la historia de la legislación española en cinco épocas, determinando que en el siglo XIX comienza la quinta época que denomina: de reforma o de retorno a la unidad[8].

Retomando el significado de lo que se entiende por código, si partimos de las palabras de Tomás y Valiente[9], este lo define como «una ley de contenido homogéneo por razón de la materia que de forma sistemática y articulada, expresada en un lenguaje preciso, regula todos los problemas de la materia unitariamente acotada». En palabras del autor, este concepto es de aplicación a los códigos europeos y americanos del siglo XIX, estando en vigor todavía gran parte de estos; es decir, esta definición encaja con el código procesal español, el cual está en vigor en pleno siglo XXI.

Continuando con lo expresado por Tomás y Valiente[10], un código «es una sola ley, elaborada por un solo legislador, promulgada en un momento dado y todos sus preceptos pertenecen, pues, a un mismo acto legislativo». Todas estas características propias de los códigos del siglo XIX sirven para cuestionar la entidad de la Ley de Enjuiciamiento Criminal española, de manera que aquel texto que irrumpía en la sociedad decimonónica y que supuso una ruptura con el sistema político-jurídico del Antiguo Régimen hoy en día está en crisis. Esta palabra indica transformación o cambio en el contexto en el que se encuentra la antigua Ley de Enjuiciamiento Criminal.

La existencia de cambios en la esfera social y política también tuvo lugar históricamente en los siglos XVIII y XIX. No hay que olvidar que se trata de una época en la que se inicia el liberalismo económico; en España, concretamente, se aprobaron diversas leyes entre 1813 y 1834 que reconocieron derechos de contenido económico que, en palabras del autor antes

---

[8] D. R. Domingo de Morato, *Estudios de ampliación de la historia de los Códigos españoles y sus instituciones sociales, civiles y políticas,* 3.ª ed., Valladolid, Libros de la Universidad y del Instituto, 1884, pp. 10 y 11, disponible en *https://bibliotecadigital.jcyl.es/.*

[9] F. Tomás y Valiente, *Manual de Historia del Derecho Español*, Madrid, Tecnos, 2007, p. 465.

[10] *Ibid.,* pp. 465 y 466.

citado, fueron sentando las bases de un nuevo régimen jurídico de las relaciones de producción y de intercambio de bienes. Es importante destacar cómo se establece la libertad para el ejercicio del comercio y de la industria, pudiéndose dedicar a estas actividades ciudadanos de todas las clases y también los extranjeros avecindados en los pueblos de la monarquía; también se reconoce la libertad de circulación por todo el territorio nacional de producciones y se suprimen las aduanas interiores[11]. De esta manera, la nueva clase social que surge tras la revolución impulsa un nuevo orden jurídico a medida que alcanza el poder político en un contexto social que difiere del establecido en el Antiguo Régimen. El nuevo orden económico que estableció las bases del liberalismo continuará a lo largo de los siglos XIX, XX y también en el siglo presente.

La libre circulación de personas, productos y servicios sigue desarrollándose ya no a nivel nacional, sino transnacional. Esta situación se pone de manifiesto de manera reciente a través del Acta del Mercado Único II presentada en 2012[12], donde se recogen las diversas medidas que la Unión debe aprobar y señala como tales: la movilidad transfronteriza de ciudadanos y empresas y la economía digital. De esta forma, el mercado se ha desarrollado y sigue evolucionando de una manera vertiginosa. Jurídicamente se reconocen derechos y libertades de carácter económico que transcienden fronteras, como el derecho a la libre circulación de los productos originarios de los Estados miembros y los productos procedentes de terceros países, o también la libre circulación de capitales entre Estados miembros y estos con terceros países con las excepciones oportunas. Por otra parte, y esto es muy relevante para el desarrollo económico de la Unión Europea, se promueve el mercado único digital a través del comercio electrónico y la administración electrónica[13].

En relación con el comercio electrónico hay que apuntar que es un tipo de compraventa que tiene su origen en la venta a distancia o venta por catálogo, es decir, se trata de un tipo de transacción que ha ido desplegándose con el paso del tiempo y que, sobre todo en el siglo XIX, tuvo una gran importancia debido a que permitía a personas que no tenían acceso directo a los productos que se ofertaban adquirirlos de manera indirecta[14].

---

[11] *Ibid.,* pp. 415 y 416.

[12] *www.europarl.europa.eu* (consultado el 8 de agosto de 2019).

[13] *Ibid.*

[14] M. T. Gimeno García, M. Á. Caballero Velasco, C. Miguel Pérez, A. M. Matas García y E. Herrera Soler, «Comercio electrónico en análisis forense», *La Biblia del Hacker*, Madrid, Anaya, 2012, pp. 553-555.

En el pasado siglo este sistema de compraventa sobre todo se desarrolló en Estados Unidos a través de la televisión y hoy en día continúa utilizándose, aunque hay que sumarle la venta en línea; esta última aparece en el presente siglo y cobra cada vez mayor importancia.

Se defiende que son numerosas las ventajas que ofrece el comercio electrónico para las empresas, entre otras: no se restringe la zona de venta, su presencia es a nivel mundial y ello se consigue a un coste muy bajo, se reducen los gastos de promoción y los beneficios por operaciones son muy elevados. A la vez también se sostiene que son muchos los beneficios para el consumidor, entre otros, la existencia de precios más ventajosos, la presencia de diferentes productos pudiendo elegir el consumidor fácilmente y la comodidad y diversidad en las formas de pago. Las cifras del comercio electrónico van en aumento; en concreto en España las ventas, de acuerdo con el Centre for Retail Research, fueron de casi 8.000 millones de euros en el año 2010[15].

Sin embargo, como consecuencia de la existencia de estas transacciones, así como por la utilización de dispositivos informáticos y, en general, por la llegada de la sociedad de la información, han proliferado las actividades ilícitas que, de acuerdo con el Anuario Estadístico del Ministerio del Interior (2011-2013), están relacionadas con los ataques contra sistemas informáticos, robo, manipulación de datos, usurpación de identidad, estafas, delitos que contravienen los derechos de propiedad intelectual y también los referidos a la posesión y distribución de pornografía infantil[16].

Volviendo al nuevo régimen jurídico, que principalmente empieza a desarrollarse en el siglo XIX, debe añadirse, siguiendo a Hernández Gómez[17], la aparición del proceso de positivación de los derechos humanos que se recoge en las Declaraciones americana y francesa de los siglos XVII y XVIII. Según la autora citada, y también de conformidad con una amplia mayoría de autores, en la fase que comienza a partir de la Revolución Francesa es cuando tiene lugar la protección de los derechos humanos, recogidos en declaraciones y en la parte dogmática de las constituciones.

Después del reconocimiento de los derechos humanos en los textos constitucionales comenzarán a regularse los sistemas de protección a nivel constitucional para, posteriormente, después de la Segunda Guerra

---

[15] *Ibid*.

[16] MINISTERIO DEL INTERIOR, *Avance de datos sobre ciber-criminalidad,* Madrid, Secretaría de Estado de Seguridad, Gabinete de Coordinación y Estudios, 2013.

[17] I. HERNÁNDEZ GÓMEZ, *Sistemas Internacionales de Derechos Humanos*, Madrid, Dykinson, 2002, pp. 23 y 24.

Mundial, garantizarlos y protegerlos por medio de mecanismos de naturaleza internacional[18]. En relación con esto último, los derechos humanos se introducen esencialmente por medio de diversos textos internacionales que se adoptan tras la Declaración Universal de los Derechos Humanos. En particular, es prioritario citar el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950 (en adelante, CEDH) y el Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966 (en adelante, PIDCP). En particular, la aplicación del CEDH, al tratarse de una norma internacional que se adopta en el ámbito del Consejo de Europa, es de especial trascendencia en nuestro Estado.

La jurisprudencia del TEDH tiene una importancia primordial tanto en la aplicación de las leyes en el Estado español como en la preparación de las nuevas normas jurídicas. A partir de la adopción del CEDH se han elaborado otros convenios de naturaleza específica que surgen a raíz de los cambios que se originan en la sociedad actual. En este sentido es necesario apuntar la ratificación por el Estado español del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. A este respecto, a nivel internacional se ha tomado conciencia de la dificultad que entraña la lucha contra los crímenes que se cometen en las redes, así como los problemas existentes para averiguar quiénes son sus autores y calibrar la entidad del delito, teniendo en cuenta, además, que la información y los datos electrónicos son volátiles[19].

Todo lo expuesto conduce a que han transcurrido casi veinte años desde que se pactó la elaboración de una nueva Ley de Enjuiciamiento Criminal por el Gobierno y por los principales partidos políticos a través del Pacto para la Reforma de la Justicia suscrito el 28 de mayo de 2001. Son numerosas las causas que fundamentan la redacción de una nueva ley procesal. A los efectos que aquí interesan, en particular, nos hallamos ante una nueva situación en la que, debido a la evolución económica y social, aparecen nuevas modalidades de delincuencia que requieren métodos de investigación adecuados, así como una nueva regulación de los actos de prueba que recojan los últimos avances tecnológicos, tal y como ya disponía el mencionado Pacto. La nueva ley procesal requiere de estudios y trabajos que examinen en profundidad los cambios que deben ser intro-

[18] *Ibid.*

[19] *Informe explicativo del Convenio sobre la Ciberdelincuencia*, disponible en *https://rm.coe.int/*.

ducidos en el enjuiciamiento penal; no obstante, como explica la exposición de motivos de la Ley 13/2015, de 5 de octubre, hay cambios que no pueden ser aplazados y que necesitan ser incorporados antes de que se promulgue la nueva Ley de Enjuiciamiento Criminal. En esta línea de urgentes reformas se sitúa la regulación de las nuevas diligencias de investigación, concretamente, el registro de dispositivos de almacenamiento masivo de información. Estos cambios están relacionados con las modificaciones que a nivel general se plantean en el proceso penal y también con las obligaciones internacionales contraídas por el Estado español. En ese marco es importante destacar que, al atribuirse la fase de instrucción penal al fiscal, el órgano jurisdiccional, en esta fase procesal, se convierte en un juez de garantías, competente para restringir, en su caso, los derechos fundamentales del investigado en el supuesto de que haya de afectarse su derecho a la privacidad; derecho que se verá afectado cuando la instrucción penal esté dirigida al descubrimiento de un hecho delictivo relacionado con el ciberdelito.

II. TEXTOS INSPIRADORES DE LA NUEVA DILIGENCIA DE INVESTIGACIÓN

Principalmente el texto jurídico que ha servido de base a la reforma introducida en la Ley de Enjuiciamiento Criminal ha sido el Convenio sobre la Ciberdelincuencia, adoptado por España mediante Instrumento de ratificación de 17 de septiembre de 2010 (*BOE,* núm. 226). De conformidad con el informe explicativo, el Convenio fue aprobado por el Comité de Ministros del Consejo de Europa en su 109.ª reunión (8 de noviembre de 2001) y fue abierto a la firma en Budapest el 23 de noviembre de ese mismo año, aprovechando la celebración de la Conferencia Internacional sobre la Ciberdelincuencia[20]. El informe pone de manifiesto los cambios que se han producido en la sociedad, concretamente la evolución que ha tenido la telefonía clásica, que se ha visto superada por el intercambio de grandes cantidades de información que incluye datos, voz, texto, música e imágenes; también la utilización del correo electrónico y el acceso a Internet, todo ello sin tener en cuenta las distancias geográficas. Junto a todos estos cambios sociales aparece lo que el informe explicativo denomina «lado oscuro», es decir, la aparición de nuevos

[20] *Ibid*.

delitos y la comisión de otros ya existentes, pero en los que se utilizan las nuevas tecnologías. Toda esa información y comunicación se extienden por todo el mundo, de manera que las fronteras no suponen un obstáculo a ese flujo de datos. Por esta razón, las soluciones que se han de dar a la utilización fraudulenta de todo ese movimiento de datos deben provenir del Derecho internacional, siempre desde el respeto de los derechos humanos en la sociedad de la información[21]. Desde ese punto de vista, Gilles Bélanger opina que, debido a la proliferación de la delincuencia, son necesarias soluciones adicionales que permitan a la justicia penal obtener en un proceso lo que se denomina «evidencia electrónica» en un marco respetuoso con los derechos humanos[22].

Flores Prada también pone de manifiesto uno de los rasgos característicos de las nuevas redes informáticas, destacando cómo los delitos informáticos superan el principio de territorialidad[23]; principio que tradicionalmente sirve para determinar la competencia del órgano instructor de la causa penal. Desde esta perspectiva, las nuevas redes informáticas se caracterizan por la supraterritorialidad, de tal forma que la información circula a gran velocidad por el espacio virtual mundial. Por este motivo, como defiende Gilles Bélanger[24], el objetivo del Convenio es poner en práctica una política penal común dirigida a proteger a la sociedad contra la ciberdelincuencia a través de una legislación adecuada y por medio de la cooperación internacional.

El llamado Convenio de Budapest recoge una serie de medidas dirigidas a la investigación penal; concretamente, su art. 19, que lleva por título «Registro y confiscación de datos informáticos almacenados», regula precisamente una serie de diligencias relacionadas con los delitos de naturaleza informática. En este sentido establece que cada Estado parte ha de adoptar las medidas legislativas y de otro carácter que resulten necesarias para facultar a las autoridades de ese Estado a registrar o acceder de una forma similar a un sistema informático o a una parte del mismo, así como a los datos almacenados en el sistema; también el acceso a un medio de almacenamiento de datos informáticos en el que puedan guardarse datos

---

[21] *Ibid*.

[22] P. Gilles Bélanger, «Derechos humanos y el Derecho penal en el ciberespacio», *Revista de la Secretaría del Tribunal Permanente de Revisión*», núm. 10 (2017), pp. 274-286.

[23] I. Flores Prada, «Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia», *RECPC, Revista de Ciencia Penal y Criminología,* núm. 17 (2015), p. 6.

[24] P. Gilles Bélanger, «Derechos humanos y el Derecho...», *op. cit.*

de esta naturaleza en su territorio. No solo los Estados parte han de legislar sobre estas medidas, sino que el Convenio enumera otras que también se han de trasladar al ordenamiento jurídico de cada Estado parte; de este modo la norma internacional establece que en las leyes internas oportunas se tendrá que prever la posibilidad de ampliar un registro cuando las autoridades que estén procediendo a su realización tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio. De igual forma, siguiendo en esta línea, se deben introducir determinadas medidas en los ordenamientos internos, a saber: confiscación de un sistema informático (o una acción similar), de una parte del mismo o de un medio de almacenamiento de datos; realización y conservación de una copia de datos informáticos; preservación de la integridad de los datos informáticos almacenados, así como hacer inaccesibles o suprimir los datos informáticos a los que se ha tenido acceso. Finalmente, el art. 19 del Convenio obliga a los Estados parte a incluir en su legislación las disposiciones necesarias para que las autoridades competentes puedan ordenar a cualquier persona que conozca el sistema informático que facilite toda la información necesaria para que se lleve a cabo el registro o la ampliación del registro a otro sistema informático.

Precisamente, las disposiciones de la Convención que son más extensas y controvertidas, en palabras de W. Brener, son las que se ocupan de la investigación y del procedimiento relacionado con el cibercrimen. A este respecto se trata de que los Estados redacten una legislación diseñada para facilitar la investigación criminal, particularmente incluyendo aquellos instrumentos que permitan la producción de evidencia electrónica, incautación legal de sistemas informáticos y recogida de datos de tráfico y de contenido, y, a su vez, el Convenio establece diversas formas de colaboración a través de la extradición de los delincuentes, intercambio de información y acceso a datos de tráfico, a lo que hay que añadir el establecimiento de un contacto que ejercerá funciones asistenciales en los procesos que traten sobre el cibercrimen[25].

Las diligencias arriba mencionadas quedan comprendidas en la Sección 2.ª del Convenio, ubicadas dentro de la sección dedicada al Derecho procesal. El alcance de estas va más allá de los delitos definidos en la Sección 1.ª, dedicada al Derecho penal. De manera que no solo se aplica-

[25] W. S. Brenner, «La Convención sobre Cibercrimen del Consejo de Europa», *Revista chilena de Derecho y Tecnología,* vol. 1, núm. 1 (2012), pp. 221-238.

rán al acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con las infracciones de la propiedad intelectual y de los derechos afines, sino que dicha Sección (procesal) se aplicará a cualquier delito cometido a través de un sistema informático o a las pruebas que se encuentren en formato electrónico. Desde este punto de vista se ha de tener presente, como apunta Gilles Bélanger[26], que la prueba digital sigue aumentando tanto en los delitos cibernéticos como en aquellos más «tradicionales» debido a que sus autores utilizan dispositivos electrónicos en la comisión de sus crímenes: secuestros, tráfico de drogas, ataques terroristas, etc. Lo que da lugar a que los investigadores y los fiscales requieran un constante acceso a la evidencia digital, siendo en algunas ocasiones complicado obtenerla por almacenarse en lugares de difícil acceso.

Teniendo en cuenta que las diligencias expuestas anteriormente son las que podrán tener lugar cuando se esté sustanciando un proceso penal en el que los hechos investigados tengan por objeto un delito cometido a través de un dispositivo electrónico, obviamente nos podemos encontrar con la necesidad de que se vean afectados los derechos del investigado. Se trata de derechos que se encuentran reconocidos en nuestro ordenamiento constitucional y también en tratados internacionales. Todo ello debido, como se ha señalado en líneas anteriores, al proceso de positivación de los derechos humanos que tuvo lugar en etapas históricas anteriores, recogiéndose tales derechos en la parte dogmática de las constituciones y después, a partir de la Segunda Guerra Mundial, en convenios internacionales. La Convención, en este aspecto, no es ajena a la existencia de este marco propio del Derecho internacional. Por esta razón, el art. 15 de la misma reconoce una serie de condiciones o salvaguardas, declarando que cada Estado parte se asegurará de que los actos que se regulan en el Convenio y que están dirigidos a la obtención de la evidencia digital respeten los presupuestos y requisitos previstos en su ordenamiento jurídico interno, garantizándose los derechos humanos y las libertades, precisamente los reconocidos en el CEDH y en el PIDCP y en otros tratados internacionales, teniéndose presente, además, el principio de proporcionalidad. En este ámbito de cumplimiento de las garantías necesarias, cada Estado deberá incluir en su ordenamiento la supervisión

[26] P. Gilles Bélanger, «Derechos humanos y el Derecho...», *op. cit.*

judicial u otro tipo de supervisión independiente de los actos procesales que se desarrollen en el proceso, así como establecer límites en su aplicación y en su ejecución. También en cada ordenamiento interno se examinarán las consecuencias de estos actos en los derechos, responsabilidades e intereses legítimos de terceros.

De esta manera la reforma operada en la ley procesal y que ha permitido la introducción de nuevas diligencias de investigación y de prueba, específicamente el registro de dispositivos de almacenamiento masivo de información, ha tenido en cuenta varios antecedentes para la regulación de esta diligencia: por un lado, el Convenio citado (donde también se recogen otros actos de investigación) se posiciona como el texto normativo más relevante debido a que obliga a los Estados parte a trasladar los mecanismos procesales reconocidos a la legislación interna; por otro, la Propuesta de texto articulado de Ley de Enjuiciamiento Criminal, elaborada por la Comisión Institucional de 2012, reunía dentro del título denominado «Contenido de las diligencias de investigación» determinados actos de investigación, entre los cuales se encontraba el «registro de dispositivos de almacenamiento masivo de información». Además, este último texto no solo ha sido tomado en consideración para la redacción de la Ley 13/2015, de 5 de octubre, sino que en el Anteproyecto de Ley de Enjuiciamiento Criminal que recientemente se ha concluido también se reconoce como documento inspirador del nuevo código procesal.

III. REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

En la Ley 13/2015, de 5 de octubre, donde se regulan las diligencias de investigación tecnológica, se recogen una serie de principios que han de ser tenidos en consideración cuando se vaya a decretar el acto de investigación oportuno. Dichos principios son: especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad. Es la propia ley la que determina los requisitos que han de estar presentes en el cumplimiento de tales principios[27]. Además, se establecen una serie de normas de aplicación común a todos los actos de investigación de carácter tecnológico[28]; a este respecto,

[27] C. Rodríguez Rubio, «La injerencia en el derecho al secreto de las comunicaciones a través de la regulación de las medidas de investigación tecnológica», *Revista Europea de Derechos Fundamentales*, núm. 28 (2016), p. 280.

[28] C. Rodríguez Rubio, «El registro de material informático: requisitos y derechos afec-

tratándose de la diligencia comentada, el órgano competente para decretarla es el propio juez de oficio o por solicitud del MF o de la Policía Judicial (en adelante, PJ). La solicitud, tal y como se regula en la ley, ha de ser completa, ya que debe reunir los requisitos que atienden a los hechos objetivos, identificación del investigado o de cualquier otro afectado, justificación de la medida, quién se ocupará de ejecutarla, el modo de ejecución y su duración. Tras la solicitud, el juez oirá al MF y decidirá en un plazo de veinticuatro horas, sin perjuicio de que el plazo pueda ser interrumpido porque sea necesario ampliar o aclarar los requisitos objeto de cumplimiento. La extensión de la resolución judicial requiere que, como mínimo, recoja: el hecho que se investiga y su calificación jurídica, indicios en los que se fundamenta la diligencia, quién es el investigado o afectado si se conociera, tipo de intervención, motivos para adoptar el acto de investigación (teniendo en cuenta los principios arriba indicados), quiénes procederán a su ejecución, duración, forma de realizarla y cuándo se informará al órgano jurisdiccional de sus resultados.

Por otra parte, la nueva ley expresa la innecesaridad de que se decrete el secreto de la instrucción, debido a que desde que se presenta la solicitud su tramitación se hará en pieza separada y secreta. También, de acuerdo con la nueva regulación, la diligencia podrá prorrogarse; asimismo, dentro de las disposiciones comunes aplicables a todos los actos de investigación tecnológica se prevé el borrado y eliminación de los registros originales cuando haya una resolución firme que ponga fin al proceso, aunque se conservará una copia bajo la custodia del letrado de la Administración de Justicia (en adelante, LAJ); no obstante, las copias que se conserven tendrán una duración determinada legalmente. Todos estos preceptos que se han comentado resultan de aplicación, como ya se ha apuntado reiteradamente, a todos los actos de investigación tecnológica; sin embargo, se ha de tener presente que habrá que integrarlos en las disposiciones que regulan específicamente «el registro de dispositivos de almacenamiento masivo de información [art. 588 *sexies a), b)* y *c)* de la Ley de Enjuiciamiento Criminal; en adelante, LECrim.]. Todas estas disposiciones comunes representan, como apunta Álvarez Sánchez de Movellán[29], «la síntesis de generosos esfuerzos jurisprudenciales y doctrinales por cubrir las carencias de unas

tados», en R. Castillejo Manzanares (dir.), *El nuevo proceso penal sin Código procesal penal,* Barcelona, Atelier, 2019, pp. 232-233.

[29] P. Álvarez Sánchez de Movellán, «La motivación de la resolución que acuerda la investigación tecnológica», en R. Castillejo Manzanares (dir.), *El nuevo proceso penal sin Código procesal penal,* Barcelona, Atelier, 2019, pp. 297-308.

actuaciones procesales sin procedimiento a seguir». A este respecto hay que partir de la base de que los actos de investigación tecnológica han carecido de un conjunto normativo que regule su funcionamiento en el proceso penal, lo que ha supuesto que la praxis por parte de los tribunales de justicia haya dado lugar a un robusto cuerpo jurisprudencial proveniente de la justicia constitucional, el Tribunal Supremo (en adelante, TS) y también del TEDH. Como opina el autor mencionado, es evidente que esa doctrina y jurisprudencia conforman «un muy buen criterio hermenéutico para la normativa finalmente aprobada». Así, lo que se verá a continuación es el modo de introducción en la LECrim. de esa jurisprudencia, dando cumplimiento, a su vez, a lo dispuesto en el Convenio sobre la Ciberdelincuencia, debido a que el tratado pretende que los actos procesales dirigidos a la obtención de la prueba digital respeten los presupuestos y requisitos de cada ordenamiento interno y al mismo tiempo se garanticen los derechos reconocidos internacionalmente y el principio de proporcionalidad.

Dentro de la diligencia denominada «registro de dispositivos de almacenamiento masivo de información», el art. 588 *sexies a)* es el primer apartado dedicado a este medio de investigación. El título del apartado indica la necesidad de que para llevar a efecto tal diligencia se requiere una resolución que motive de manera individual el acto. De esta forma, cuando haya de practicarse un registro domiciliario y se prevea «la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos» el juez de instrucción en su resolución deberá explicar las razones que permiten que los agentes facultados puedan acceder a los dispositivos. Concretamente, el nuevo artículo de la ley procesal dispone que «la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos».

Esta resolución individualizada que legitima la injerencia se ha reconocido en la jurisprudencia. Concretamente, en la STS 204/2016, de 10 de marzo, se dice que la intervención de un ordenador requiere de un acto jurisdiccional habilitante y especificamente se establece lo siguiente: «Y esa resolución no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentren instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferente, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como

sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías». También en un pronunciamiento más reciente, la STS 311/2020, de 15 de junio, expone lo siguiente: «El acceso al contenido de la información alojada en un equipo informático requiere una habilitación judicial específica, distinta de la concedida para una entrada y registro». Particularmente esta sentencia viene a decir que el acceso a un ordenador necesita de una justificación singularizada y distinta de la que se requiere para una entrada y registro en domicilio, ya sea en el mismo auto o en resoluciones independientes.

Evidentemente, el contenido de este precepto [art. 588 *sexies a)*] se ha de poner en relación con la diligencia de entrada y registro de un domicilio; en general, para el registro de dispositivos electrónicos en un domicilio es necesario conjugar ambas diligencias. De esta manera, cuando existan indicios de encontrar en un domicilio efectos o instrumentos del delito u otros objetos que sirvan para su descubrimiento o comprobación (arts. 546 y 550 LECrim.), el juez competente dictará una resolución motivada con la finalidad de efectuar la entrada y proceder al registro para aprehender los objetos que puedan estar relacionados con su comisión. Precisamente, en la resolución que dicte el órgano jurisdiccional competente tendrá que justificar la aprehensión de los dispositivos informáticos en los que se pueda encontrar información relacionada con el hecho delictivo; es decir, es necesario, como se ha apuntado más arriba, tener presente en la realización de la diligencia los preceptos procesales en los que se regula la entrada y registro en un lugar cerrado.

En este sentido, se trata de llevar a cabo determinadas diligencias que limitan los derechos fundamentales del afectado por tales actos de investigación: por un lado, cuando se procede a decretar la entrada en un domicilio se ve restringido el derecho a la inviolabilidad del domicilio y, por otro, se verán restringidos el derecho a la intimidad y el derecho a la protección de datos de carácter personal si la finalidad es el registro domiciliario con el fin de aprehender los objetos relacionados con el crimen. Al tratarse de medidas limitativas de derechos, su adopción, en palabras de Armenta Deu[30], requiere el cumplimiento de determinados presupuestos, sobre todo teniendo en cuenta el reconocimiento constitucional de tales derechos, así como su garantía en diversos tratados internacionales. En

[30] T. Armenta Deu, *Lecciones de Derecho Procesal Penal,* Madrid, Marcial Pons, 2016, p. 177.

definitiva, y siguiendo lo defendido por la autora[31], será necesario que la restricción del derecho esté prevista legalmente, que la medida limitativa se decrete en el marco de un proceso y, finalmente, que se haya adoptado conforme al principio de proporcionalidad.

Como se ha apuntado en líneas anteriores, se han de integrar las normas referidas a la entrada y registro de lugar cerrado con la nueva ley que regula las diligencias de carácter tecnológico. En este aspecto es importante tener en consideración que en la diligencia primero mencionada (entrada y registro en lugar cerrado), la Ley 13/2005, de 5 de octubre, no ha introducido novedades en su regulación; por esta razón, en cuanto al concepto de domicilio resulta de aplicación el art. 554 LECrim. donde se recogen los lugares que tienen esta condición[32]. Respecto al concepto de domicilio, es de interés recordar que no existe un solo concepto, de manera que las leyes civiles, administrativas o penales le atribuyen un contenido diferente. Desde el punto de vista procesal, el domicilio tiene una estrecha relación con la intimidad; así, de acuerdo con la Sentencia 22/1984, de 17 de febrero, del Tribunal Constitucional, el domicilio «es un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima»[33].

Por otro lado, el art. 554 LECrim., ya mencionado, fue modificado por Ley 37/2011, de 10 de octubre, de medidas de agilización procesal, por el que se añadió un nuevo apartado mediante el cual se estableció el domicilio de las personas jurídicas como aquel espacio que constituye su centro de dirección, ya sea su domicilio social o un establecimiento dependiente, o aquellos otros lugares en los que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros. En este aspecto, este último apartado, introducido en el art. 554 LECrim., relaciona claramente el concepto de domicilio con el concepto de privaci-

---

[31] *Ibid.,* pp. 177 y 178.

[32] Se reputa domicilio para los efectos de los artículos anteriores (art. 554 LECrim.): «Los palacios reales, estén o no habitados por el monarca al tiempo de la entrada o registro.

El edificio o lugar cerrado, o la parte de él destinada principalmente a la habitación de cualquier español o extranjero residente en España y de su familia.

Los buques nacionales mercantes.

Tratándose de personas jurídicas imputadas, el espacio físico que constituya el centro de dirección de las mismas, ya se trate de su domicilio social o de un establecimiento dependiente, o aquellos otros lugares en que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros».

[33] C. Rodríguez Rubio, «La entrada y registro domiciliario y la interceptación de las comunicaciones postales y telefónicas», en *Desafíos jurídicos-sociales del nuevo milenio*, Madrid, Servicio de Publicaciones Universidad Rey Juan Carlos, 2000, p. 361.

dad. En relación con aquellos lugares que no se identifican con el domicilio de las personas físicas, el apartado cuarto del precepto citado ha servido para aclarar el concepto de domicilio, aunque antes de su introducción en la ley procesal ya había habido pronunciamientos sobre su significado; así, en Sentencia de 7 de octubre de 2008 (asunto *Mancevschi c. Moldavia*), el TEDH manifestó cómo reiteradamente el despacho de un abogado ha sido considerado hogar en sentido amplio y cómo su registro es considerado una injerencia en la vida privada, viéndose así afectado el art. 8 del CEDH[34].

Para la realización del registro de dispositivos de almacenamiento informático que se encuentren en un domicilio se necesitará que el juez competente decrete la entrada; a este respecto, es de aplicación el art. 18 CE en el que se reconoce la inviolabilidad del domicilio, no pudiéndose entrar en él si no hay consentimiento o autorización judicial, salvo el delito flagrante. Así, a falta del consentimiento del titular (el art. 551 LECrim. entiende que hay consentimiento cuando se realizan los actos necesarios para que se efectúe la entrada y no se invoca el derecho a la inviolabilidad), deberá procederse a la entrada mediante resolución judicial. En cuanto al tipo de resolución, el propio texto constitucional no expresa qué forma adoptará la decisión judicial, pero la ley procesal exige un auto fundado donde se recoja cuál es el edificio o el lugar donde se ha de practicar y la autoridad o funcionario que vaya a realizarlo; además, siguiendo los presupuestos que se han de tener en cuenta cuando se restringe un derecho fundamental, la medida decretada, es decir, la entrada, ha de cumplir con el principio de proporcionalidad, ya que se trata de un acto limitador de derechos. En la resolución dictada el juez deberá establecer la extensión de la medida de investigación, indicando los dispositivos electrónicos y, en su caso, los archivos informáticos que serán registrados, así como el modo de conseguir que la información obtenida mediante el registro esté completa y debidamente protegida [art. 588 *sexies c)*, apartado primero] con el fin de realizar, si fuera procedente, un dictamen pericial.

---

[34] Art. 8. Derecho al respeto a la vida privada y familiar.

«Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia está prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Cuando se pretende entrar en un domicilio con la finalidad de registrarlo es común que la resolución judicial venga precedida de una solicitud por parte de la Policía Judicial. A su vez, esta petición policial será previa a una actividad investigadora que determine la existencia de datos que permitan al juez de instrucción decretar la entrada. La solicitud de la Policía necesitará de un informe que sirva para determinar cuál es el domicilio que será examinado, a quién afectará, el delito investigado y los efectos que podrán ser hallados y que están relacionados con el delito[35], entre estos podrán ser confiscados los ordenadores personales y otros dispositivos electrónicos.

Por otra parte, el nuevo precepto [art. 588 *sexies a),* apartado 2] determina que la confiscación de un dispositivo electrónico cuando se esté efectuando un registro domiciliario no permite, sin más, el acceso a su contenido, aunque con posterioridad podrá ser autorizado por el juez competente. Este precepto puede inducir a dudas sobre su significado, pero se podrá interpretar de manera que, decretada la entrada en un domicilio para realizar un registro y no habiéndose justificado las razones por las que corresponde acceder a la información existente en los dispositivos que se puedan localizar durante este, los agentes podrán requisarlos para, posteriormente, conseguir la autorización judicial que permita conocer su contenido. Esto último respondería a lo dispuesto en el Convenio sobre la Ciberdelincuencia, ya que se pretende incluir en los ordenamientos internos la supervisión judicial, así como las limitaciones que correspondan en los actos de aplicación y ejecución de los actos procesales dirigidos a obtener la evidencia digital.

En cuanto al juez que ha de dictar la resolución para proceder a la entrada y registro, el art. 546 LECrim. establece que será el que conozca de la causa. No obstante, la ley procesal permite que el juez instructor atribuya la diligencia a la autoridad o a la PJ, siendo posible también que, si el edificio se encontrara fuera del territorio del tribunal, se asigne su práctica al del lugar donde se encuentre el edificio objeto del acto de investigación. La citada resolución, tratándose de domicilios de particulares, se ha de comunicar a su titular. A este respecto, el art. 566 LECrim. determina que si no es encontrado se comunicará al encargado y, en su defecto, se hará la notificación a cualquier otra persona mayor de edad que se encuen-

[35] A. de Peray Barjés, «La diligencia de entrada y registro en lugar cerrado», en P. Martín García (dir.), *La actuación de la policía en el proceso penal*, Madrid, Marcial Pons, 2006, pp. 182-183.

tre en el domicilio, dando preferencia a los familiares del interesado. Por último, el precepto se refiere a que si no se halla a nadie se extenderá una diligencia firmada por dos vecinos.

A juicio de Peray Barjés[36], los testigos podrán ser, si no hay vecinos, policías municipales, nacionales o autonómicos que acompañen a los funcionarios que intervengan en la investigación y en el registro. No obstante, se ha de tener presente que el art. 566 LECrim. determina que en todo registro estará el LAJ del órgano jurisdiccional que lo hubiera autorizado; literalmente el precepto dice lo siguiente: «El registro se practicará siempre en presencia del secretario del Juzgado o Tribunal que lo hubiere autorizado, o del secretario del servicio de guardia que lo sustituya, quien levantará acta del resultado de la diligencia y de sus incidencias que será firmada por todos los asistentes. No obstante, en caso de necesidad el secretario judicial podrá ser sustituido en la forma prevista en la Ley Orgánica del Poder Judicial». Sobre este precepto es preciso apuntar que, a pesar de lo dispuesto, cuando se comunique la resolución judicial no se necesitará la intervención de los dos vecinos debido a que, de conformidad con la Ley Orgánica del Poder Judicial (en adelante, LOPJ), los LAJ ejercen la fe pública con exclusividad y plenitud; así, en el ejercicio de esta función no precisan de la intervención adicional de testigos (art. 453.4 LOPJ). En relación con la intervención del LAJ, hay que apuntar que su presencia puede ser en parte determinante para considerar válido el acto de investigación. En ese marco, en la Sentencia 311/2020, de 15 de junio, el recurrente en casación solicita la nulidad del registro que afectaba al dispositivo informático, previa entrada en su domicilio, porque cuando proporcionó las claves de acceso a su ordenador no se encontraba asistido de su abogado. A este respecto, el TS declara que no se puede proceder a la nulidad pretendida por diversas razones, entre ellas las siguientes: «*a)* Según consta en el acta de entrada y registro, la comunicación de las claves se hizo en presencia del letrado de la Administración de Justicia. *b)* No consta ni se ha alegado que hubiera ningún tipo de intimación en la obtención de la colaboración ni que se realizara en un ambiente de coacción ambiental».

Cuando el juez haya acordado la entrada y el registro del domicilio se adoptarán las medidas de vigilancia necesarias para evitar, en su caso, la sustracción de los instrumentos, efectos u objetos relacionados con el hecho delictivo (art. 567 LECrim.), es decir, será prioritario tomar las precauciones oportunas para que no se extraigan los dispositivos informáticos. Acer-

[36] *Ibid.,* p. 569.

ca del riesgo de que los dispositivos sean sustraídos o manipulados hay que apuntar que la nueva ley opta principalmente por la copia de su contenido, siempre en condiciones que garanticen la autenticidad e integridad de los datos, aunque si los aparatos electrónicos constituyen el objeto o instrumento del delito o existen otras razones que lo justifiquen podrán ser incautados [art. 588 *sexies c),* apartado 2]. Una vez que se han adoptado las medidas de seguridad necesarias tiene lugar el acceso al domicilio, para lo cual se podrá utilizar el uso de la fuerza si es necesario (art. 568 LECrim.).

Posteriormente tendrá lugar el registro y para este fin se requiere la presencia del interesado o de su representante y, en su defecto, se podrá llevar a cabo ante la comparecencia de un familiar que sea mayor de edad; si finalmente no se pudiera contar con la asistencia de estos sujetos se requerirá la comparecencia de dos vecinos. El precepto que regula en presencia de quién se ha de realizar el registro (art. 566 LECrim.) además añade la asistencia imprescindible del LAJ, estableciendo, como se indica en líneas anteriores, que este podrá ser sustituido en la forma prevista en la LOPJ. Respecto a este apartado hay que señalar que la intervención del LAJ explícitamente se introdujo en la LECrim. por medio de la Ley 22/1995, de 17 de julio; con su introducción se pretendía garantizar la asistencia de este funcionario público a la diligencia de entrada y registro debido a que la jurisprudencia del Tribunal Supremo consideraba que el acto era nulo si el secretario judicial no estaba presente en su realización[37].

Por otra parte, también es preciso apuntar que, como se ha podido comprobar, la ley procesal permite que el secretario pueda ser sustituido tal y como se prevé en la LOPJ. Al respecto, el art. 282 de esta ley facultaba a los secretarios para que habilitaran a uno o más oficiales para la realización del acto, siendo estos los responsables de la autenticidad de los actos que acreditaran. Sin embargo, este precepto fue derogado por Ley Orgánica 19/2003, de 23 de diciembre; de este modo, en el momento presente se ha de partir de lo dispuesto en el art. 452.1 *in fine* LOPJ, donde se pone de manifiesto que las funciones de los LAJ no pueden ser objeto de delegación ni de habilitación, salvo lo que expresamente determina el art. 451.3 LOPJ. Así, se puede afirmar que en caso de necesidad el LAJ podrá ser sustituido por el funcionario del Cuerpo de Gestión Procesal y Administrativa cuando sea procedente entrar en un domicilio y llevar a cabo un registro con el fin de acceder a los dispositivos informáticos y no hubiera suficientes LAJ. Esta circunstancia se dará cuando se haya

[37] C. Rodríguez Rubio, «La entrada y registro domiciliario...», *op. cit.,* p. 364.

de proceder a varias entradas y registros que se hayan acordado por un solo órgano jurisdiccional de la Audiencia Nacional y tengan que realizarse simultáneamente.

De conformidad con la Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos, el medio idóneo para garantizar la identidad de los dispositivos será su reseña por el LAJ en el acta de registro cuando haya sido incautado con motivo de este. También, de acuerdo con la circular mencionada, se debe precintar el dispositivo y ponerlo a disposición del juez; por otra parte, siempre que se vaya a dejar sin efecto el precinto (por ejemplo, para realizar el clonado) se tendrá que hacer bajo la fe del LAJ y tras su terminación deberá ser de nuevo precintado.

Por otro lado, cuando se pretende la confiscación de un equipo informático o de otros dispositivos y se entra con esta finalidad en un domicilio, la diligencia que se pretende acometer está relacionada con el cuerpo del delito debido a que en su realización los agentes facultados proceden a recoger o requisar los instrumentos del hecho delictivo. No hay que olvidar que el lugar donde se comete el crimen ofrece una gran información sobre cómo se ha ejecutado el delito, instrumentos u objetos utilizados, identidad del autor e identidad de la víctima. Como sostiene Gómez Colomer, en torno a la escena del crimen: «Lo más importante es aplicar una buena técnica de investigación y saber descubrir los vestigios dejados por el criminal y atender a los hallazgos que se produzcan de manera adecuada»[38]. Respecto a la diligencia del cuerpo del delito, nos encontramos ante un acto de investigación que en su mayor parte no ha tenido modificaciones legales desde su redacción original, lo que puede dificultar su aplicación en el proceso. A pesar de ello y siguiendo al autor citado[39], las normas legales y, en su caso, las técnicas policiales de investigación deben atender a la conservación de todos los objetos, vestigios y demás elementos que puedan encontrarse en el lugar donde se haya cometido el delito, con el objetivo de realizar el correspondiente informe pericial, así como su información al órgano jurisdiccional y a las partes.

En criminología la escena del delito cobra una especial importancia porque el investigador podrá obtener información muy relevante sobre el crimen cometido[40]. Esta circunstancia fue puesta de manifiesto por

---

[38] J. L. Gómez Colomer, «El procedimiento preliminar: los actos de investigación», en *Derecho Jurisdiccional,* vol. 3, *Proceso Penal*, 24.ª ed., Valencia, Tirant lo Blanch, 2016, p. 176.

[39] *Ibid.*

[40] *www.estudiocriminal.eu* (30 de septiembre de 2019).

Edmond Locard en su libro *Manual de técnica policiaca,* donde expuso que «es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia». Este autor sostenía que en la escena del crimen hay un intercambio de materiales físicos, de manera que el autor del delito deja vestigios o evidencias y a su vez se lleva otras consigo del lugar de los hechos; es lo que se ha llamado principio de intercambio[41]. Esta situación, que puede tener lugar en crímenes de distinta naturaleza, la expresa con claridad Rámila Díaz al defender que cuando una persona entra en contacto con un medio, algo de él queda en el lugar y algo del lugar queda en la persona. La autora lo compara con una imagen muy elocuente, a saber: al caminar por la playa, con seguridad se nos quedarán granos de arena en los pies, y, a su vez, nosotros dejaremos huellas en la arena[42].

Este principio es trasladable a los elementos que son utilizados en la comisión de un delito informático. A este respecto, los agentes facultados pueden encontrar en el registro domiciliario equipos o dispositivos que constituyen el cuerpo del delito y que de una forma muy significativa podrán evidenciar los hechos criminales, el autor o autores y la víctima; por esta razón, Ferro Veiga apunta que dentro de la informática forense y desde el punto de vista de la actuación de las Fuerzas y Cuerpos de Seguridad la metodología a seguir debe estar dirigida a recoger el máximo de pruebas y a perjudicar lo menos posible a la víctima. Concretamente, tratándose de prueba digital, se debe obtener la máxima información sobre el tipo, lugar y conexiones de cualquier sistema de ordenadores; además, como ocurre en el escenario de cualquier hecho delictivo, se han de tomar las debidas precauciones para no contaminar los vestigios, es decir, no se deberá contaminar la escena digital por medios físicos o electrónicos[43].

Retomando la realización de la diligencia, hay que tener en cuenta que la presencia de los distintos sujetos que han de concurrir a su práctica es un deber que impone el art. 569 LECrim. al determinar que si el interesado, su representante, los familiares o los testigos se resisten a presenciar el acto serán juzgados por un delito de desobediencia grave a la autoridad; además esta circunstancia no impide que se lleve a efecto el acto de investigación. Por su parte, la Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos,

---

[41] *Ibid*.

[42] J. Rámila Díaz, *La ciencia contra el crimen*, Nowtilus, 2010, libro electrónico.

[43] J. M. Ferro Veiga, *Manual de investigación privada*, CreateSpace, 2013, libro electrónico.

al comentar lo relativo a la resolución judicial que permite la realización del registro dispone que las exigencias del registro domiciliario no se pueden extender al registro de dispositivos al tratarse de dos diligencias distintas; por esta razón en el registro domiciliario será necesaria la presencia del interesado en los términos establecidos en la LECrim., no siéndolo para acceder a la información del dispositivo. Por otro lado, y continuando con lo previsto en la ley procesal, si en la ejecución del registro no se encontraran los dispositivos informáticos que se pretendieran hallar ni aparecieran indicios sospechosos, el interesado podrá solicitar que se expida un certificado del acto practicado (art. 569 LECrim. *in fine*).

También siguiendo lo establecido para la entrada y registro en domicilios particulares, se practicará de día, aunque también podrá tener lugar durante la noche si se dan estas circunstancias, a saber: en caso de urgencia si fuera necesario y cuando haya comenzado de día y, no habiendo finalizado, el interesado o su representante permitan que continúe durante la noche (arts. 570 y 550 LECrim.). Si no fuera así y se diera esta última situación se habrán de tomar las medidas necesarias para evitar la sustracción de los objetos, esto es, de los dispositivos objeto de registro. Además, si resulta necesario el registro podrá ser suspendido, adoptándose las medidas de vigilancia que se precisen (art. 571 LECrim.). En la realización del registro es posible, como también adelanta el Convenio de Budapest, que el sujeto o sujetos que lo realizan consideren razonadamente que la información buscada se encuentra en otro sistema informático o en una parte de él, en este caso se podrá ampliar el registro siempre que se pueda acceder de conformidad con el sistema inicial o porque haya disponibilidad respecto de este. No obstante, se determina legalmente la necesidad de autorización judicial salvo que el juez ya lo hubiera autorizado desde el principio, lo que da lugar a que se pueda prever esta circunstancia y el órgano jurisdiccional lo acuerde desde el comienzo de la investigación. Por otro lado, la ampliación puede ser llevada a cabo por la PJ o el fiscal si existen motivos de urgencia. Con relación a esta exigencia, habrá que apuntar que la urgencia, como más adelante se verá, alude a la situación en la que hay un riesgo de pérdida de la información; en este sentido los datos informáticos son inestables por lo que puede ser necesaria una actuación rápida de la Policía. Sin embargo, esta actuación tiene que ser comunicada inmediatamente al juez, en todo caso en un plazo de veinticuatro horas, poniendo en su conocimiento la forma y el resultado del acto. Tras la comunicación el órgano jurisdiccional deberá decidir si respalda la medida en un plazo de setenta y dos horas desde que se ordenó.

Asimismo, y con el fin de poder acceder a la información contenida en los ordenadores personales o en otros aparatos electrónicos, los sujetos intervinientes (autoridades y agentes) podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos que les faciliten la información que sea necesaria, siempre que no sea algo desproporcionado para el afectado bajo apercibimiento de incurrir en un delito de desobediencia [art. 588 *sexies c),* apartado 5]. Esta orden no podrá dirigirse al investigado o al encausado debido a que podría verse afectado su derecho a no declarar contra sí mismo, así como a su derecho a no confesarse culpable (art. 588 *sexies c)*, apartado 5, en relación con el art. 24.2 CE). Tampoco podrá darse esta orden a las personas dispensadas de la obligación de declarar por razón de parentesco y a aquellas que han de guardar el secreto profesional de conformidad con el art. 416.2 LECrim. Después de la finalización de la diligencia y teniendo en cuenta el acto de entrada y registro en lugar cerrado (art. 572 LECrim.), se dejará constancia de los sujetos que han intervenido, de los incidentes que hayan tenido lugar, del comienzo y fin de la diligencia, del orden utilizado en el registro y de los resultados obtenidos.

Sin duda la finalidad del registro de aparatos electrónicos es llevar a cabo un informe pericial con el objeto de recoger la información que sirva para el descubrimiento del delito. Así, la pericia, siguiendo a Moreno Catena, estaría compuesta por un informe en el que se recogerían los hechos relevantes para el proceso y se realizaría por personas con especiales conocimientos; se trataría, a juicio del autor, de un acto materialmente similar al acto de prueba[44]. En la LECrim. se encuentran numerosas disposiciones (arts. 456 a 485) que resultan de aplicación a la pericia; sin embargo, nos encontramos ante un determinado acto de investigación que por su naturaleza requiere de una serie de actuaciones que en esencia no se encuentran reguladas en la ley procesal. No se puede olvidar que nos encontramos ante lo que se ha denominado evidencia o prueba digital, en la que se incluyen archivos, información, datos, vídeos, fotografías, correos almacenados, que responde a los cambios que han tenido lugar en una época reciente debido al desarrollo de las nuevas tecnologías. De esta manera deberán utilizarse en la investigación las herramientas forenses[45] que sean precisas para la averiguación de los datos contenidos en los dispositi-

[44] V. Moreno Catena, *Actos de investigación* en *Derecho Procesal Penal*, Valencia, Tirant lo Blanch, 2019, p. 262.

[45] En relación con las herramientas forenses, *vid.* J. M. Ferro Veiga, *Manual de investigación privada*, *op. cit.*

vos electrónicos, además es necesario que las Fuerzas y Cuerpos de Seguridad sigan una serie de pasos que garanticen la integridad de la información examinada.

A juicio de Ferro Veiga, se ha de establecer una metodología aplicable a la informática forense en el examen del material informático[46]. Se ha de llevar a cabo una sucesión de actuaciones que se inicia con la identificación, con el objeto de comprobar el hecho delictivo por requerimiento de la autoridad judicial, y que terminará con la redacción del informe pericial. En esta sucesión de actos habrá distintas fases; de esta manera habría que preparar y planificar las herramientas y las técnicas que se van a utilizar, comprobando que los equipos estén en buen estado y no contaminados. Por otro lado, siguiendo al autor citado[47], la planificación debe estar dirigida a recoger el mayor número de pruebas y a minimizar el impacto sobre la víctima.

En relación con esto último, hay que poner de relieve que en los delitos de posesión y distribución de pornografía infantil, el Convenio de Budapest proporciona a los Estados parte un instrumento dirigido a la investigación criminal y, a su vez, una herramienta para la protección de los menores debido a que entre las medidas que se han de introducir en los ordenamientos internos se encuentra la que consiste en hacer inaccesible o suprimir los datos informáticos a los que se ha tenido acceso, de esta forma el daño al menor podrá reducirse evitando la difusión de las imágenes dentro y fuera del territorio nacional. En este sentido, la Convención sobre el Cibercrimen del Consejo de Europa se constituye como el único instrumento internacional que vincula a los Estados parte; además es una guía para los países de nuestro entorno si se quiere lograr una legislación nacional contra el ciberdelito[48]. Evidentemente puede ser un instrumento útil en la lucha contra el abuso y la explotación infantil, ya que los informes muestran que decenas de miles de niños son víctimas de estos hechos, siendo además frecuente que se trate de un delito de naturaleza trasnacional, estando en constante evolución[49].

Siguiendo con las actuaciones encaminadas a obtener la información precisa sobre el hecho delictivo y continuando con lo apuntado por Ferro Veiga, tratándose de la prueba digital hay que lograr la máxima información sobre el tipo, lugar y conexiones de cualquier sistema de ordena-

---

[46] *Ibid.*
[47] *Ibid.*
[48] *https://www.coe.int* (21 de agosto).
[49] *Ibid.*

dores[50]. Hay que asegurarse de que se toman las precauciones necesarias para no contaminar la escena digital, ya sea por medios físicos o electrónicos. Este aspecto es importante porque se puede alterar o incluso perder la información contenida en el dispositivo. Así, será muy importante respetar la cadena de custodia. Por otro lado, y en relación con el examen de la información, esta podrá tener lugar en el laboratorio, lo que es preferible a juicio del autor citado, o en el lugar donde se encuentre el dispositivo. No obstante, siempre es importante realizar la copia o el clonado de la evidencia digital y proceder a la firma digital.

De acuerdo con la Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos informáticos, cuando el dispositivo no se confisque y se deje en manos del investigado se realizarán dos copias: una garantizará el contenido del dispositivo y la segunda servirá para realizar el análisis que exija la investigación. El LAJ será el encargado de garantizar la primera copia. También hay que tener en cuenta que además de dispositivos electrónicos pueden ser examinados repositorios telemáticos; en relación con estos últimos, es útil recordar que se puede acceder a ellos desde otros dispositivos que no estén en poder del investigado. Por esta razón, la Circular 5/2019 apunta a que las claves para acceder a estos servidores tendrán que ser cambiadas por decisión judicial, con la finalidad de que no sean modificados. Además, deberá realizarse un volcado de información bajo la fe del LAJ que será quien garantizará el origen y su contenido.

Siguiendo al autor antes citado, en el examen de la información hay que cumplir con la cadena de custodia; asimismo, hay que cumplir con la autorización judicial que justifica el registro. Cuando se proceda al análisis, en primer lugar se realizará un estudio preliminar de los dispositivos examinados en cuanto a sus características y posteriormente se pasará a analizar e interpretar los datos que se obtengan. Al final de lo que se tratará es de redactar un informe por escrito donde queden plasmados los actos realizados, los hallazgos, su interpretación y las conclusiones de los expertos[51]. En relación con el examen del dispositivo, en la STS 311/2020, de 15 de junio, se ha expuesto lo siguiente: «Es necesario que cuando se realice la entrada y registro domiciliario se identifique debidamente el ordenador intervenido, debido a que una falta de control administrativo o jurisdiccional sobre las piezas de convicción del hecho

[50] J. M. Ferro Veiga, *Manual de investigación privada*, *op. cit.*
[51] *Ibid.*

delictivo puede dar lugar a equívoco sobre lo que realmente fue analizado. Lo contrario podría implicar una más que visible quiebra de los principios que definen el derecho a un proceso con todas las garantías». En este sentido también se ha pronunciado la STS 167/2020, de 19 de mayo. De esta manera puede suceder que no se haya nombrado de la misma forma el modelo de ordenador en el acta de diligencia de entrada y registro y en el informe pericial, pero si la marca y el número de serie coinciden, este dato individualiza al aparato de forma absoluta.

Para concluir con este apartado habría que añadir que en una futura Ley de Enjuiciamiento Criminal habrá que regular, dentro de la prueba pericial, el modo de incorporar el informe realizado en la instrucción dentro de la fase de enjuiciamiento. A este respecto, la propuesta de texto articulado de la LECrim., elaborada por la Comisión Institucional creada por Acuerdo del Consejo de Ministros de 2 de marzo de 2012, puede servir de referencia. Al tratarse de un texto articulado es posible encontrar ciertos preceptos que pueden ser un anticipo de lo que finalmente podrá regularse en el futuro. Así, se hace referencia a que en la fase de juicio oral el Tribunal examinará, entre otras cosas, los soportes de datos y otras piezas de convicción que ayuden a esclarecer los hechos y que obren en la pieza principal (art. 462.1). Además podrán ser exhibidos, a solicitud del fiscal o de cualquiera de las partes, durante el interrogatorio que se haga a los testigos, al encausado o en la prueba pericial (art. 462.2). Tras la práctica de los medios probatorios de naturaleza personal el Tribunal preguntará a las partes acusadoras si desean hacer alguna pregunta sobre los soportes de datos y demás fuentes de prueba que consideren importantes para apoyar sus peticiones (art. 463.1); lo mismo ocurrirá con las pruebas personales de la defensa en relación con la prueba de descargo (art. 463.2).

IV. APREHENSIÓN Y REGISTRO DE DISPOSITIVOS ELECTRÓNICOS CONFISCADOS FUERA DEL DOMICILIO DEL INVESTIGADO

La nueva regulación de las diligencias de naturaleza tecnológica permite también la incautación de dispositivos electrónicos fuera del domicilio de la persona que está siendo investigada. En este contexto, el dispositivo debe ser requisado en algún lugar que no constituya el domicilio de la persona física o de la persona jurídica a la que se atribuya la comisión del crimen, es decir, de esta manera la LECrim. (art. 588 *sexies*) prevé el acceso

a la información que se halle en un dispositivo siempre y cuando se haya iniciado un proceso penal y se haya determinado en fase de instrucción la persona o personas que aparecen, en un primer momento, como presuntos responsables de un hecho delictivo. El acceso a la información que contenga el dispositivo requerirá necesariamente una resolución judicial, en particular un auto, que justifique las razones por las que se accede a la información que contiene el dispositivo electrónico.

El TS mantiene una posición nítida al respecto. Así, en la Sentencia 204/2016, de 10 de marzo, pronunciamiento importantísimo en la materia que se examina y que requiere una atención especial en los párrafos posteriores, se declara en relación con la resolución judicial lo siguiente: «Esta autorización será precisa tanto en los supuestos en los que los teléfonos móviles se ocupen en un registro domiciliario, como en los incautados fuera del domicilio del investigado». El motivo por el que se precisa autorización judicial es porque en los dispositivos electrónicos se encuentra información que afecta a la privacidad del investigado. Concretamente, el pronunciamiento se expresa en los siguientes términos: «La razón de ser de la necesidad de esta autorización con carácter generalizado es la consideración de estos instrumentos como lugar de almacenamiento de una serie compleja de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones a través de sistemas de mensajería, por ejemplo, tuteladas por el art. 18.3 CE; contactos o fotografías, por ejemplo, tuteladas por el art. 18.1 CE que garantiza el derecho a la intimidad; datos personales y de geolocalización que pueden estar tutelados por el derecho a la protección de datos, art. 18.4 CE)». También hay otras sentencias anteriores del TS que han tratado la materia que es objeto de estudio. Singularmente, la Sentencia 342/2013, de 17 de abril, hace referencia a que el acto de la PJ, como acto unilateral, no legitima el acceso al contenido del ordenador del imputado y ello por las razones siguientes: los dispositivos de almacenamiento masivo son más que una pieza de convicción que una vez aprehendida queda expuesta al control de los investigadores. El contenido de este tipo de dispositivos no es simplemente un instrumento donde se recibe información relacionada con la intimidad y la protección de datos, sino que el dispositivo normalmente albergará información ligada al derecho a la inviolabilidad de las comunicaciones.

Por otra parte, los lugares físicos en los que se pueden encontrar dispositivos electrónicos y que, a su vez, no pueden ser considerados domicilios pueden ser muy variados. En general, se tratará de lugares cerrados que no constituyen el domicilio de la persona investigada; así, podemos citar:

vehículos, almacenes y locales, entre otros. Son numerosas las ocasiones en las que el TS se ha pronunciado sobre la entrada en estos lugares. Siguiendo a Torres Morato[52], en relación con el registro de vehículos, la doctrina tradicional sobre su registro se encuentra en la Sentencia del Tribunal Supremo de 31 de octubre de 1981, de la que se puede extraer lo siguiente: el vehículo no constituye domicilio ya que no se puede predicar su inviolabilidad; su registro no precisa de autorización judicial; es posible trasladar el vehículo a un lugar distinto para llevar a cabo el registro, sin que ello afecte a la regularidad de la prueba, y, por último, el contenido de los derechos fundamentales está delimitado por la propia Constitución y por las disposiciones de naturaleza internacional.

Asimismo, y continuando con los lugares que pueden ser objeto de registro con el fin de que se pueda incautar un dispositivo electrónico, los departamentos de literas de tren que tienen carácter colectivo tampoco se reputan domicilio a los efectos de que se pueda hacer valer el derecho a la inviolabilidad del domicilio. Siguiendo al autor citado[53] y en virtud de la STS de 28 de diciembre de 1994, en su interior no es posible desarrollar la intimidad ni tampoco puede el viajero excluir a las personas que se encuentran en él; de esta forma estas serían las dos características principales que sirven para determinar si la privacidad está en juego cuando se procede al registro de un lugar cerrado en el que podrá ser requisado un aparato electrónico, esto es, la posibilidad de que la persona pueda desplegar su intimidad en ese ámbito cerrado, así como el poder de rechazar a otros sujetos en ese lugar.

En definitiva, en los supuestos en los que el aparato electrónico es aprehendido por la PJ, aunque la confiscación haya tenido lugar fuera del domicilio del investigado, como se ha mencionado con anterioridad, se precisa para tener acceso a la información contenida en estos de autorización judicial. Lo que se requiere legalmente es la puesta en conocimiento por la Policía de la incautación ante la autoridad judicial. El juez, tras la comunicación, tendrá que valorar si el acceso a la información es indispensable para la averiguación del delito y de los delincuentes. En este sentido, el órgano competente tendrá que decidir si la diligencia de investigación es pertinente para el descubrimiento de los hechos delictivos y de su autor (art. 299 LECrim.); también tendrá que comprobar la concurrencia

---

[52] M. Á. Torres Morato, «Registro de automóviles y objetos cerrados», en E. de Urbano Castrillo y M. Á. Torres Morato, *La prueba ilícita penal, Estudio jurisprudencial*, Navarra, Aranzadi Thomson Reuters, 2010, pp. 302-303.

[53] *Ibid.,* pp. 308-309.

de los principios que han de estar presentes para la aplicación del acto de investigación, esto es, principio de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad.

V. ACCESO DE LA POLICÍA JUDICIAL A LOS DISPOSITIVOS SIN PREVIA RESOLUCIÓN JUDICIAL

Cuando se accede a un dispositivo, como puede ser un ordenador personal o un teléfono móvil, se pueden ver afectados distintos derechos fundamentales, todos ellos garantizados en el art. 18 CE y también reconocidos en el art. 8 CEDH. Estos derechos están estrechamente relacionados con la privacidad, de manera que en el precepto constitucional se garantiza el derecho a la intimidad personal y familiar, el derecho a la propia imagen, la inviolabilidad del domicilio, el secreto de las comunicaciones y el derecho a la protección de datos de carácter personal. Se trata de derechos que pueden verse restringidos en el marco de una investigación criminal, y en numerosas ocasiones cuando tiene lugar el acceso a un aparato electrónico no solo se puede ver invadido uno de los derechos reconocidos en el art. 18, sino que pueden ser varios los afectados por la actuación de la PJ.

A este respecto, el TC ha considerado en Sentencia 70/2002, de 3 de abril, que el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que la reducción que se haga de aquel sea necesaria para lograr un fin constitucionalmente legítimo, sea proporcionado y se respete el contenido esencial del derecho. Esta línea ha sido mantenida por el TC durante años, expresándose en este sentido en varios de sus pronunciamientos, a saber: SSTC 98/2000, de 10 de abril; 186/2000, de 10 de julio, y 156/2001, de 2 de julio. Hay que poner de manifiesto que, como se ha apuntado con anterioridad, son diversos los derechos reconocidos en el art. 18 CE y que todos ellos están relacionados con el derecho a la privacidad. No obstante, las garantías que el legislador ofrece a unos y otros no son exactamente las mismas. En este aspecto, la Constitución española no prevé expresamente que la injerencia en el derecho a la intimidad requiera de autorización judicial. Así lo ha reconocido el TC en la Sentencia 70/2002, de 3 de abril, ya citada: «En cuanto a la necesidad de autorización judicial, a diferencia de lo que ocurre con otras medidas restrictivas de derechos fundamentales que puedan ser adoptadas en el curso penal (como la entrada y registro en domicilio del art. 18.2 CE o la intervención

de las comunicaciones del art. 18.3), no existe en la Constitución reserva absoluta de previa resolución judicial». A pesar de ello, en la STC 37/1989, de 15 de febrero, se estableció que la restricción del derecho a la intimidad era «*solo posible por decisión judicial»,* aunque sin descartar la posibilidad de que en determinados casos y con la conveniente habilitación legislativa, tales actuaciones pudieran ser dispuestas por la Policía Judicial.

En relación con lo dicho, es importante mencionar la Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre registro de dispositivos y equipos informáticos, cuando examina el registro policial de dispositivos, porque declara cómo la ley que regula las nuevas diligencias de investigación no considera de manera individualizada los derechos fundamentales que pueden resultar afectados por el registro de un dispositivo, sino que partiendo de determinadas sentencias del TS (STS 204/2016, de 10 de marzo) realiza un tratamiento unitario, reconociéndose actualmente el llamado derecho al entorno virtual de la persona. En palabras de Gómez Colomer, el medio de investigación examinado supondría un desarrollo específico dentro del proceso penal del derecho al secreto de las comunicaciones, viéndose también afectados el derecho a la protección de datos y el derecho a la privacidad (intimidad y a la propia imagen). El propio autor sostiene que, ante esta complejidad dogmática, se habla modernamente del «derecho al propio entorno virtual» (STS 342/2013, de 17 de abril), siendo un derecho de nueva generación y que integraría todos los derechos mencionados[54]. En ese marco, partiendo de la sentencia citada por la Circular y que venimos examinando (STS 204/2016, de 10 de marzo), se establece ese concepto actual mencionado por Gómez Colomer[55]. Específicamente, el TS se expresa de la siguiente manera: «Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos».

---

[54] J. L. Gómez Colomer, «Los actos de investigación garantizados (II)», en *Derecho Jurisdiccional,* vol. 3, *Proceso Penal*, 24.ª ed., Valencia, Tirant lo Blanch, 2016, p. 262.

[55] *Ibid.*

Son numerosas las ocasiones en las que la PJ ha tenido acceso a la información contenida en un ordenador personal o en un teléfono móvil en el ámbito de la realización de las diligencias dirigidas al descubrimiento del delito y de su autor. Particularmente, es importante poner de manifiesto, por la gravedad de los hechos y por su análisis por parte del TEDH, el asunto *Trabajo Rueda c. España,* habiendo recaído Sentencia por parte del Tribunal Europeo el 30 de mayo de 2017[56]. En relación con los hechos, estos se remontan a 2007, cuando un técnico informático a través de una denuncia comunica a la Policía la posesión de material pornográfico por parte de un ciudadano español. La denuncia presentada se debe a la entrega de un cliente de un equipo informático para su reparación; con este fin, el informático procedió a su arreglo y al llevar a cabo esta actuación descubrió que en una de las carpetas se encontraba material pornográfico de menores. El técnico entregó el equipo a la Policía y esta procedió al examen del contenido de la computadora, accediendo a la carpeta «mis documentos» y al programa de intercambio y de compartición de ficheros eMule; después de sus indagaciones, el ordenador fue entregado a la PJ experta en informática y posteriormente se comunicaron los hechos al juez.

En este asunto, la Policía había tenido acceso directo a la información contenida en el ordenador personal del cliente que había acudido al técnico, circunstancia que se puede valorar, desde el punto de vista policial, como diligencia de prevención o primeras diligencias que realiza la Policía para la averiguación del delito. En este sentido, el art. 282 LECrim. determina que la Policía tiene como obligación averiguar los delitos públicos que se cometan en su territorio, practicar las diligencias necesarias para su comprobación y descubrir a los delincuentes; también recoger todos los efectos, instrumentos o pruebas del delito cuando exista riesgo de su desaparición.

Igualmente, el art. 13 de la Ley Procesal establece que dentro de las diligencias de prevención se encuentra la consignación de pruebas que puedan desaparecer. No obstante, nos encontramos ante un acto de la Policía que afecta a un derecho fundamental: el derecho a la intimidad personal. Por esta razón, el abogado del acusado en el juicio defendió la vulneración del derecho a la intimidad de su cliente porque la Policía había accedido al contenido de su ordenador y además había procedido a la grabación de los archivos. La Audiencia Provincial declaró la ausencia de violación del derecho a la vida privada del acusado porque él mismo no

[56] C. Rodríguez Rubio, «El registro de material informático...», *op. cit.,* p. 226.

había restringido el acceso de terceras personas a sus ficheros. El recurso contra la sentencia fue desestimado debido a que el Tribunal entendió que la intromisión en su intimidad había sido consentida por el recurrente, ya que entregó el equipo sin ninguna limitación y se hallaron los ficheros en una carpeta compartida con otros usuarios del programa eMule.

Finalmente, el condenado recurrió en amparo ante el TC por la vulneración de su derecho a la intimidad personal y a la presunción de inocencia, tesis que fue avalada por el fiscal que intervenía en la causa. En la sentencia que puso término al proceso constitucional, el TC aludió a la STC 70/2002, de 3 de abril, declarando que el acceso al contenido del equipo informático necesita de previo consentimiento de su propietario o de autorización judicial que respete, al igual que la intervención policial, el principio de proporcionalidad. De acuerdo con lo mantenido por el TC, había existido una intromisión no consentida en el derecho a la vida privada del recurrente en amparo. El TC entendió que la intervención policial no contaba con resolución judicial previa; no obstante, esta circunstancia es una excepción permitida en la jurisprudencia española. En palabras del TC, hubo una serie de circunstancias que dieron lugar a que la actuación de la Policía fuera necesaria, cumpliéndose el principio de proporcionalidad. Estas circunstancias se justifican basándose en que el poseedor del material pornográfico no se hallaba detenido por lo que era posible que se procediera al borrado de datos desde otra ubicación o de los que se pudieran encontrar en otro lugar; también era importante que la Policía investigara si había otros sujetos implicados, incluso también si se había cometido un delito de abuso de menores.

En la sentencia del TC se presentó un voto particular discrepante que defendía que el acceso al ordenador personal se había realizado sin autorización judicial previa y ante la inexistencia de una situación de urgencia que justificara la intervención de la Policía. El asunto tratado fue llevado ante el TEDH, y mediante Sentencia de 30 de mayo de 2017, el Tribunal Europeo manifestó la vulneración del art. 8 CEDH, declarando la dificultad existente en considerar la urgencia que había conducido a la Policía a intervenir el ordenador personal del interesado sin autorización judicial, debido a que no existía riesgo de desaparición de ficheros al ser un ordenador intervenido y retenido por la Policía, entendiendo el TEDH que se podría haber esperado a obtener una resolución judicial que se podría haber logrado con relativa rapidez[57].

[57] *Ibid.,* pp. 232-233.

En este asunto encontramos una discrepancia de pronunciamientos entre el TC y el TEDH. El TC, en el caso comentado, alude a su relevante Sentencia 70/2002, de 3 de abril. Esta última resolución tiene un gran peso (como se puede observar a lo largo de este trabajo) en lo relativo al derecho a la intimidad y a su restricción por los poderes públicos. En dicho pronunciamiento, referido a la detención, pero que debe tenerse en cuenta en el caso examinado por afectar al derecho controvertido, se dice lo siguiente: «La regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que solo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir esta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial para que sea el juez quien los examine. Esta regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En estos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad». Teniendo en cuenta los hechos que se suceden y la jurisprudencia del TC, nos hallamos ante una situación en la que se enjuicia de distinta forma la urgencia y la necesidad de la injerencia: por un lado, el TC reconoce que hay una intromisión en el derecho a la vida privada, también que efectivamente no hay resolución judicial previa, pero, no obstante, defiende la existencia en la jurisprudencia española de que haya una excepción a la regla establecida; por otro, el TEDH considera que no hay una situación de urgencia, que no había riesgo de perder la prueba debido a que el ordenador se encontraba en poder de la PJ y que se podría haber obtenido una resolución judicial en poco tiempo.

En relación con los registros que tienen lugar por la Policía y que se realizan sin previa resolución judicial, la ley que regula las nuevas diligencias de investigación dedica un apartado a los requisitos que han de cumplirse para que se lleve a cabo el acto de investigación. Así, el art. 588 *sexies c),* apartado 4, determina que la Policía podrá llevar a efecto el examen directo del dispositivo incautado con el fin de conocer su contenido; a este respecto deberán estar presentes varios presupuestos, a saber: tendrá que tratarse de una situación urgente, lo que significa que el acceso a la información es necesario e inaplazable; deberá apreciarse un interés constitucional legítimo, es decir, que se trate de un valor o principio reconocido constitucionalmente; además el acto debe ser comunicado inme-

diatamente al juez competente, en todo caso en un plazo de veinticuatro horas, mediante escrito motivado y exponiendo las razones que justifican la medida, la actuación realizada, la forma y su resultado; finalmente, el órgano jurisdiccional se pronunciará sobre la adecuación de la medida en un plazo de setenta y dos horas desde que fue ordenada.

Es cierto que el precepto comentado puede plantear dudas sobre su aplicación por los últimos términos empleados, debido a que se refiere a que la medida debe ser confirmada por el juez en un plazo de setenta y dos horas desde que fue ordenada, lo que implica que pueda presentarse la duda de si la medida fue mandada por el juez; sin embargo, cabe entender que nos encontramos ante una situación en la que la Policía, por las circunstancias concurrentes de urgencia y de necesidad, accede a la información del dispositivo sin autorización judicial previa. Es una situación reconocida por el TC y que el propio TEDH reconoce si se dan los presupuestos apuntados. Desde este punto de vista y teniendo en cuenta que la nueva ley trata los derechos afectados por este acto de investigación de manera conjunta, no individualizada, se trataría de un registro sin autorización judicial, pero que posteriormente se podrá ver convalidado si reúne los requisitos y es aprobado judicialmente. El TC en Sentencia 70/2002, de 3 de abril, ya expuso los requisitos que habían de estar presentes cuando la PJ procedía a realizar un acto que supusiera una injerencia en el derecho a la intimidad sin que previamente se hubiese dictado resolución judicial. A este respectó declaró: «La valoración de la urgencia y necesidad de la intervención policial ha de realizarse *ex ante,* y es susceptible de control judicial *ex post,* al igual que el respeto del principio de proporcionalidad. La constatación *ex post* de la falta de presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales».

En este sentido, los delitos relativos a la posesión y distribución de pornografía infantil son susceptibles de ser investigados a través de esta diligencia[58], pudiéndose dar la circunstancia de que la Policía, sin previa autorización judicial, acceda al dispositivo si se dan los presupuestos exigidos legalmente, a saber: debe tratarse de una situación urgente que requiere necesariamente que se realice la diligencia, porque de otro modo podría perderse la información; en este sentido es preciso tener en cuenta que los datos de naturaleza informática son volátiles y, por tanto, es posible su des-

[58] *Ibid.,* pp. 229 y 234.

aparición. Por otra parte, la Policía debe apreciar un interés constitucional legítimo, concretamente los menores están amparados por las normas internacionales que velan por sus derechos (art. 39.4 CE). En esta materia, los derechos del niño están reconocidos en la Convención de las Naciones Unidas sobre los Derechos del Niño adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989, siendo esta norma internacional uno de los cuerpos normativos inspiradores del Convenio de Budapest.

Por otro lado, retomando la diligencia de entrada y registro en lugar cerrado, tal y como aparece regulada en la LECrim., es necesario mencionar el art. 553, artículo modificado por Ley Orgánica 4/1988, de 25 de mayo, porque permite a la Policía, de propia autoridad, detener y registrar un lugar o un domicilio donde se oculte o refugie una persona contra la cual haya un mandamiento de prisión, también cuando esta cometa un delito flagrante, así como cuando es inmediatamente perseguida por la autoridad y se refugia en alguna casa, o cuando se trata de un presunto responsable de un delito de bandas armadas o elementos terroristas. En estos casos se podrán ocupar los efectos e instrumentos que se hallasen y que pudieran guardar relación con el delito.

En todas estas situaciones, que son excepcionales, la Policía al realizar el registro podrá requisar los ordenadores personales o dispositivos electrónicos, pues la ley procesal permite su ocupación. Una vez efectuado se ha de dar conocimiento al juez competente justificando su realización y exponiendo sus resultados; también habrá que indicar si se han llevado a cabo detenciones, quiénes han intervenido y los incidentes que hayan tenido lugar. Tras la aprehensión de los dispositivos por la Policía es posible preguntarnos si se puede acceder directamente a su contenido, ya que se trata de circunstancias excepcionales y no hay resolución judicial previa. La respuesta entendemos que ha de venir dada por la regulación que hace la nueva ley de la diligencia que se viene comentando. A este respecto, el nuevo precepto parte de la existencia de una autorización individualizada para que pueda practicarse el acto de investigación tanto si se procede al registro del domicilio como cuando se registra este lugar y no se ha autorizado el registro previamente, determinándose que haya autorización con posterioridad; también es necesaria cuando se realiza fuera del domicilio del investigado. Y habría que añadir que en aquellos supuestos en los que concurra una situación de urgencia y haya un interés constitucional legítimo, la Policía podrá acceder directamente al contenido cumpliendo posteriormente con los requisitos que más arriba se han comentado y que se recogen en el art. 588 *sexies c),* apartado 4, LECrim.

Por otro lado, la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (en adelante, LPSC), recoge una serie de potestades generales de la policía de seguridad para llevar a cabo el mantenimiento y restablecimiento de la seguridad ciudadana. Estas actuaciones resultan relevantes en el tema que es de nuestro interés, porque en el ámbito de sus competencias, la Policía puede llevar a cabo la aprehensión de dispositivos electrónicos. La acción de la Policía puede tener lugar en las vías, lugares o establecimientos públicos con el objeto de prevenir los delitos especialmente graves o que generen alarma social y también con la finalidad de descubrir y averiguar a sus autores. Para ello podrán realizar detenciones, así como proceder a la recogida de instrumentos, efectos o pruebas, y para tal fin podrá establecer controles en esos lugares para identificar a las personas, registrar vehículos y también proceder a un control superficial de efectos personales (art. 17.2 LPSC). Cuando con ocasión de una detención policial se proceda a la confiscación de un dispositivo electrónico, de acuerdo con la Circular 5/2019 antes citada, la PJ deberá proceder a identificar en el acta que levante y que aparecerá en el atestado que se redacte el dispositivo confiscado con la finalidad de que no haya duda sobre cuál es el aparato electrónico del que surgen las pruebas y el dispositivo aprehendido.

También la misma Ley, en su art. 18.2, permite que la Policía proceda a la ocupación temporal de objetos, instrumentos, medios de agresión e incluso de armas con licencia con la finalidad de prevenir la comisión de un crimen o si se pusiera en peligro la seguridad de bienes o de personas. Cuando la Policía realice estas actuaciones y, concretamente, proceda a un registro y lleve a cabo la aprehensión de algún objeto o instrumento levantará acta que deberá ser firmada por el interesado, salvo que se niegue, en cuyo caso se hará costar esta circunstancia. Por otro lado, el apartado primero del precepto anteriormente citado también faculta a la Policía para que realice comprobaciones en personas, bienes y vehículos que se encuentren en vías, lugares y establecimientos públicos con el objeto de impedir que se porten diversos objetos que supongan un riesgo y que puedan ser utilizados para cometer un delito o alterar la seguridad ciudadana, si hay indicios de que puedan encontrarse en esos lugares, en cuyo caso serán intervenidos. Por último, conviene tener presente que la Policía dentro de sus competencias puede realizar registros corporales externos y superficiales cuando haya indicios racionales que permitan, tras su realización, hallar instrumentos, efectos u objetos relevantes en el ejercicio de las funciones de investigación y de prevención del delito.