La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información

The protection of personal data in the register of massive information storage devices

Miren Josune Pérez Estrada[1]
Universidad del País Vasco – España
mirenjosune.perez@ehu.eus
http://orcid.org/0000-0001-7402-4863

Resumen: El objeto de este trabajo es poner de manifiesto los problemas que plantea la investigación criminal cuando se analizan instrumentos tecnológicos en la averiguación del delito. En concreto, se estudia cómo afecta al derecho fundamental a la protección de los datos personales la prueba que se ha obtenido, con motivo de la investigación criminal, mediante el análisis de los datos contenidos en los dispositivos de almacenamiento masivo de la información. Se analiza el tratamiento jurídico que se da a la protección de los datos personales como parte de lo que se ha venido a denominar por la jurisprudencia "protección del entorno virtual" y las consecuencias jurídicas que tiene en el proceso penal. En definitiva, se quiere advertir cuáles son los efectos que tiene en el proceso penal la prueba que se ha obtenido vulnerando el derecho fundamental a la protección de los datos personales.

Palabras clave: Protección de datos de carácter personal; entorno virtual; dispositivos de almacenamiento masivo de información; garantías procesales; prueba ilícita.

Abstract: *This paper studies the affection of the personal data in the criminal investigation of the evidences of the mass storage devices of the information.*

[1] Profesora Adjunta de Derecho Procesal (acreditada Agregada). Departamento de Derecho Público. Facultad de Derecho. Sección Bizkaia.

The protection that jurisprudence gives to the protection of personal data is studied as "protection of the virtual environment" and also the possible consequences that it has in the criminal process, at the moment in which the judge evaluates the evidence, if the personal data of the researched have been achieved by violating the fundamental right to the protection of personal data.

Keywords: *Protection of personal data; virtual environment; massive information storage devices; procedural guarantees; evidence obtained violating fundamental rights of the process.*

Sumario: Introducción; 1. Configuración del derecho fundamental a la protección de los datos personales; 2. Límites del derecho fundamental a la protección de los datos personales; 3. La protección del derecho fundamental de los datos personales frente a los nuevos métodos de investigación tecnológica en el proceso penal; 3.1. Aproximación normativa; 3.2. Los dispositivos de almacenamiento masivo de información; 3.3. Protección del derecho al entorno virtual; 3.4. Extensión y límites del registro de dispositivos de almacenamiento masivo de la información; 3.5. Acceso a los datos personales por la policía judicial y consentimiento del interesado; Conclusiones: Efectos de la prueba obtenida mediante registro de dispositivos de almacenamiento masivo de la información vulnerando el derecho fundamental a la protección de los datos de carácter personal; Referencias bibliográficas.

Introducción

La investigación tecnológica en la averiguación del delito es compleja pero se ha convertido, en la actualidad, en imprescindible en la instrucción de la mayoría de los delitos para la averiguación de los hechos y la autoría de los mismos. El uso de técnicas tradicionales de investigación cede ante los resultados que proporcionan las nuevas técnicas de investigación. Las evidencias electrónicas prevalecen en la información que se encuentra disponible o almacenada en dispositivos de almacenamiento y constituyen fuente de prueba para poder acreditar el hecho investigado. Los dispositivos de almacenamiento masivo constituyen

efectos del delito en sí mismos pero, además, será necesario acceder a la información que contienen para la averiguación de los hechos. Precisamente, es en este acceso que, por otra parte, es inevitable donde se produce una lesión o afectación del derecho fundamental a la protección de los datos personales, además de a otros derechos como la intimidad y al secreto de las comunicaciones. Lo relevante será comprobar si la limitación al derecho fundamental es de suficiente entidad como para verse afectada la prueba obtenida y, en su caso, las consecuencias que tenga en el proceso penal.

Cómo afecta al derecho fundamental a la protección de los datos personales la investigación del material informativo que contienen los dispositivos de almacenamiento masivo de la información es el objetivo del trabajo. Partiendo del hecho que los datos personales sólo se pueden proteger desde el ejercicio de la facultad de autodeterminación individual[2] el problema que acucia a este derecho es el propio desconocimiento del peligro que entraña el acceso por terceros a los datos personales que no afectan a la vida íntima de la persona. Esta consideración de los datos, al margen de la esfera íntima, hace que no se repare en su utilización y manipulación que, inevitablemente, conlleva el control de la vida personal del individuo. No obstante, este derecho tiene como límites la propia investigación de un hecho delictivo aunque es necesario que esta investigación se realice de la manera más respetuosa al derecho que protege los datos personales porque sólo así la prueba obtenida en la investigación de los hechos criminales podrá ser válida en el proceso penal. Estudiamos en este trabajo el tratamiento procesal que, en la actualidad, se otorga a la protección de los datos personales como parte de lo que se ha venido a denominar por la jurisprudencia "protección del entorno virtual". Se analiza la regulación jurisdiccional nacional con motivo de la modificación

[2] MURILLO DE LA CUEVA, Pablo Lucas. La Constitución y el derecho a la autodeterminación informativa. *Cuadernos de Derecho Público*. Madrid, n. 19 – 20, 2003, pp. 36 – 39, apuesta por el nombre de autodeterminación informativa (también se conoce a este derecho como habeas data, libertad informática o protección de los datos personales) acuñado por el Tribunal Constitucional Federal alemán, sentencia de 15 de diciembre de 1983 y que entiende que expresa la sustancia del derecho: "El control de uno mismo sobre la información personal que le afecta y sirve para proyectarlo frente a la informática o frente a cualquier tecnología" (p. 39).

efectuada por la Ley Orgánica 7/2015, de 21 de julio que añade, por el art. único 36, el Capítulo I bis, el art. 236 bis al decies, sobre la Protección de datos de carácter personal en el ámbito de la Administración de Justicia y se examina si resulta adecuada para proteger los datos personales que se obtienen en una investigación criminal o en la fase de la instrucción procesal. Finalmente, se concluye exponiendo las consecuencias que tienen en el proceso penal los datos personales del investigado obtenidos vulnerando este derecho fundamental, en concreto, las consecuencias que tiene en la valoración de la prueba de los datos personales de la persona investigada que se han obtenido vulnerando este derecho fundamental.

1. Configuración del derecho fundamental a la protección de los datos personales

El derecho fundamental a la protección de los datos de carácter personal es un derecho de los que se han venido a denominar "tercera generación" y está en íntima relación con la incidencia negativa de las Tecnologías de la Información y de las Comunicaciones (TIC) en el ejercicio de los derechos fundamentales[3]. La protección de los datos

[3] Autores como PÉREZ LUÑO, Antonio Enrique (autor imprescindible por ser el iniciador en España de los estudios sobre esta materia), Intimidad y protección de datos personales: del "habeas corpus" al "habeas data. In: GARCÍA SAN MIGUEL, Luis (coord.). *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos, 1992, pp. 36 – 45, lo califican como la "tercera generación de derechos humanos". Se trata del "derecho a la paz, los derechos de los consumidores, el derecho a la calidad de vida, o la libertad informática". También del mismo autor *Del Habeas Corpus al Habeas Data*. Conferencia impartida en el XIV Curso de Informática y Derecho. Centro Regional de la UNED, Extremadura, 1990,, p. 154 – 155, sostiene que "...nos hallamos ante una tercera generación de derechos humanos complementadora de las fases anteriores, referidas a las libertades de signo individual y a los derechos económicos, sociales y culturales. De este modo, los derechos y libertades de la tercera generación se presentan como una respuesta al fenómeno de la denominada "contaminación de las libertades" (*liberties pollution*), término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías.

Disponible en http://egov.ufsc.br/portal/sites/default/files/6_16.pdf. Fecha acceso: 07de junio de 2018.

personales no se recoge expresamente en el art. 18.4 CE[4] pero sí se contiene en él y ello como protección contra las amenazas a la dignidad, identidad, libertad e intimidad de las personas[5]. Estamos ante un derecho que pone de manifiesto la necesaria protección de los datos personales frente al tratamiento automatizado de los mismos que afecta al control de "nuestras vidas y personalidad" [6]; por lo tanto, el acento lo debemos poner en el "control" ejercido como poder sobre la otra persona, como disposición o manejo de la vida de las demás personas a través de sus datos personales.[7]

---

4 El punto 4. del art. 18 establece: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

5 La protección de los datos personales es el principal aspecto de la tutela de los derechos de las personas frente al uso de la informática a la que se refiere el art. 18.8 de la Constitución. De esta manera lo manifiesta MURILLO DE LA CUEVA, Pablo Lucas. La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Jurídicos (Nueva época)*. Madrid, n. 104, 1999. Sobre la importancia de la protección de los datos frente al uso de la informática y autónomo de la protección del derecho a la intimidad, PIÑAR MAÑAS, José Luis. La protección de datos personales y ficheros automatizados. In: ROMEO CASABONA, Carlos María (coord.). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada: Comares, 2006, pp. 153-167.

6 La línea jurisprudencial pionera en la tutela fundamental de los datos personales la marca la Sentencia del TC 254/1993, de 20 de julio, (BOE núm. 197, de 18 de agosto de 1993). Su importancia radica en que abre una línea jurisprudencial que conduce, posteriormente, al reconocimiento de este derecho fundamental y la conexión que establece entre el Convenio nº 108, de 28 de enero de 1981, del Consejo de Europa, sobre el tratamiento automatizado de los datos de carácter personal y el propio art. 18.4 CE, en atención al propio art. 10.2 CE (" Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España."). Supera de esta manera la doctrina de la Sala tercera del TS que los trata únicamente de principios. Estas consideraciones aparecen ampliamente argumentadas por el autor MURILLO DE LA CUEVA, Pablo Lucas, La Constitución y el derecho a la autodeterminación informativa, op. cit., p. 31.

7 MURILLO DE LA CUEVA, Pablo Lucas, La Constitución y el derecho a la autodeterminación informativa, op. cit., p. 36. Pone el autor de manifiesto que "...el riesgo específico que implica la informática es el control sobre las vidas de los demás que permite la captación incontrolada de información

El desarrollo del art. 18.4 CE se realiza con la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)[8], derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (LOPD) que vino a transponer la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En la actualidad, con motivo de la aplicación directa desde el 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), se ha elaborado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[9].

---

personal...". "Es decir, la recopilación y el tratamiento automatizado de datos sobre los más variados aspectos de nuestras actividades..., de nuestras vidas y de nuestra personalidad... Y todo ello con la particularidad de que el resultado de esas elaboraciones, en tanto que producto de un tratamiento de datos, puede que ni siquiera sea verdad".

8 Fruto, además, de la ratificación del Convenio núm. 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (entró en vigor el 1 de octubre de 1985).

9 BOE núm. 294, de 6 de diciembre de 2018. Junto a dicha normativa destacan los siguientes instrumentos jurídicos: La Carta de Derechos Fundamentales de la Unión Europea recoge, en su art. 8, la protección de datos de carácter personal y el Tratado de Lisboa, Declaración nº 21, firmado el 12 de diciembre de 2007, dispone la posibilidad de establecer normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en el ámbito de la cooperación judicial y policial. Podemos ver en este tema a GUTIÉRREZ ZARZA, María Ángeles.-, Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea y El Tratado de Funcionamiento de la Unión Europea. In: GUTIÉRREZ ZARZA, María Ángeles (coord.). *Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal*. Madrid: La Ley, 2012.

En el ámbito jurisdiccional la protección de los datos personales se encuentra también regulada en la legislación orgánica, Ley Orgánica del Poder Judicial (LOPJ) en su última modificación efectuada por la Ley Orgánica 7/2015, de 21 de julio añade por el art. único 36 el Capítulo I bis, el art. 236 bis al decies, sobre la Protección de datos de carácter personal en el ámbito de la Administración de Justicia. Se ha superado la regulación anterior incompleta y obsoleta que venía establecida por el Reglamento 1/2005, de aspectos accesorios a las actuaciones judiciales, aprobado por Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial y por la LOPJ, art. 230.5 LOPJ.

2. Límites del derecho fundamental a la protección de los datos personales

El derecho fundamental a la protección de los datos no es absoluto. La limitación de su ejercicio viene dada de forma genérica en el art. 10.1 CE cuando se residencia en el orden público y la paz social[10]. El TC señala como límite del derecho fundamental a la protección de los datos personales, entre otros, la averiguación, persecución y castigo del delito[11]. El resto de derechos fundamentales y bienes jurídicos protegidos constitucionalmente actúan también como límite al ejercicio del derecho fundamental, en atención a la necesidad, proporcionalidad y a que sea "respetuoso con el contenido esencial del derecho fundamental restringido"[12].

---

[10] Art. 10.1 CE: "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social."

[11] Lo recuerda la STC 292/2000, en su FJ 9: "En cuanto a los límites de este derecho fundamental no estará de más recordar que la Constitución menciona en el art. 105 b) que la ley regulará el acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas" (en relación con el art. 8.1 y 18.1 y 4 CE) ..."

[12] De esta manera lo recoge el FJ 11 de la STC 292/2000: "...en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos

De manera más específica los límites al derecho a la autodeterminación informativa los encontramos entre los derechos que protege el art. 24 CE y que comprende: tutela judicial efectiva, derecho a un proceso con todas las garantías, derecho de defensa[13] y el derecho a la prueba. Por lo tanto, debemos entender que el derecho a la protección de los datos personales del investigado o encausado, ie., el poder de control, de disposición de sus datos personales que se traduce en la imposición a terceros determinados deberes de hacer: "el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos" cede o "presenta ciertas limitaciones" en el proceso penal con el fin de conseguir llevar a buen término una investigación penal[14]. De esta manera lo establece el art. 236 quáter LOPJ: "De conformidad con lo dispuesto en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre[15], no será necesario el consentimiento del interesado para que los Tribunales procedan al tratamiento de los datos en el ejercicio de la potestad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud del propio Tribunal, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.

En el Espacio de Libertad, Seguridad y Justicia (ELSJ) de la Unión Europea los límites a este derecho fundamental vienen impuestos por la Directiva (UE) 2016/680 del Parlamento europeo y del consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que

---

fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución..."

13 Una dimensión más amplia de los límites al derecho fundamental a la protección de datos en el proceso penal lo encontramos en Autor, 2018.

14 STC 254/1993, de 20 de julio, FJ 7.

15 Se debe entender referida a la normativa actual LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

se deroga la Decisión Marco 2008/977/JAI del consejo. La Directiva establece las normas sobre protección de los datos personales de las personas físicas respecto del tratamiento que realicen las autoridades con motivos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. En los supuestos de delincuencia transnacional la cooperación, basada en el principio de reconocimiento mutuo, entre autoridades policiales y judiciales resultará crucial para el esclarecimiento del delito grave y así se garantiza, a través de la Directiva, el intercambio de datos personales por parte de estas autoridades.

3. La protección del derecho fundamental de los datos personales frente a los nuevos métodos de investigación tecnológica en el proceso penal

3.1. Aproximación normativa

La reforma de la Ley de Enjuiciamiento Criminal (LECr) por la LO 13/2015, de 5 de octubre, de modificación de la LECr para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [16] supuso dar cobertura legal a las medidas de investigación tecnológica[17]. De esta manera, se regulan las diligencias de investigación de intervención de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos. Se trata de los Capítulos IV a X del Título VIII ("De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución") que se añade por el

[16] BOE núm. 239, de 6/10/2015.

[17] Anteriormente, no existía una regulación concreta de esta materia en la LECr. En los supuestos de acceso a la prueba electrónica se aplicaban por analogía preceptos de la LECr y la amplía doctrina jurisprudencial que si se había desarrollado en esta materia

arts. únicos13 a 19 de la Ley Orgánica 13/2015, de 5 de octubre, arts. 588 bis a 588 octies.

La nueva regulación pretende dotar de mayor eficacia al derecho procesal a la vez que se procura que se actúe con pleno respeto a las garantías del proceso, sobre todo, cuando se pueden afectar derechos fundamentales de la persona, reconocidos en el art. 18 LECr[18]. Y es que la regulación de estas diligencias de investigación había sido ampliamente demandada por la doctrina[19] y jurisprudencia; en ese sentido, la STC 145/2014 recuerda la necesidad de una habilitación legal en los supuestos de injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas.[20]

Con la reforma de la LECr se cumple con las obligaciones que resultan de la ratificación del Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001[21], que se aplica a la obtención de pruebas electrónicas[22] y se ha dado cobertura legal a las medidas de investigación

---

[18] Véase la Exposición de Motivos, apartado IV.

[19] Sobre este tema, véase, entre otros, ETXEBERRIA GURIDI, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal*. Madrid: Agencia de protección de Datos, Premio Protección de datos Personales, 1998, pp. 22; CASTILLEJO MANZANARES, Raquel. *Hacia un nuevo proceso penal*. Madrid: La Ley, 2010y; BANACLOCHE PALAO, Julio; ZARZALEJOS NIETO, Jesús. Las diligencias de investigación restrictivas de los derechos fundamentales. In: *Aspectos fundamentales del Derecho Procesal Penal*. Madrid: La Ley, 3ª ed., 2015.

[20] La Sala Segunda del TC en su sentencia 145/2014 (ECLI:ES:TC:2014:145), FJ 7.

[21] BOE núm. 226, de 17 de septiembre de 2010.

[22] Art. 14.2 c) Convenio de Budapest sobre Ciberdelincuencia. La prueba electrónica o en soporte electrónico la define SANCHÍS CRESPO, Carolina. La prueba en soporte electrónico. In: GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián, (coords.). (, *Las tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Navarra: Thomson Reuters-Aranzadi,, 2012, p. 713, como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal". Con carácter general, la prueba en el proceso penal cabe definirla como "la actividad procesal, de las partes (de demostración) y del juez (de verificación), por la que se pretende lograr el convencimiento psicológico del juzgador acerca de la verdad de los datos alegados al proceso". De esta manera, la describe . BARONA VILAR, Silvia.

tecnológica, siguiendo la jurisprudencia de la Sala de lo Penal del TS. Destacamos entre la numerosa doctrina jurisprudencial las siguientes sentencias del TS: STS 250/2017, de 5 de abril[23], sienta la doctrina general sobre los presupuestos necesarios para la autorización de la interceptación de las comunicaciones telefónicas y telemáticas, STS 272/2017, de 18 de abril[24], sobre la utilización de dispositivos técnicos de captación de la imagen con motivo de la nueva regulación de la LECr y STS 786/2015, de 4 de diciembre[25], sobre registro de dispositivos de almacenamiento masivo de información, en este caso acceso al contenido de ordenadores; importa resaltar en esta sentencia la doctrina jurisprudencial sobre el derecho al propio entorno virtual.[26].

En el art. 588 bis LECr[27]se contiene la regulación de las disposiciones comunes a las medidas de investigación tecnológica que marcan los principios rectores de la autorización judicial que se otorgue al efecto. Estos principios disponen que la misma habrá de ser dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Además, en los arts. 588 ter a 588 quinquies se regulan la interceptación de las comunicaciones telefónicas y telemáticas (Capítulo V), Captación y grabación de comunicaciones orales mediante la utilización de dispositivos

La prueba (I). In: MONTERO AROCA, Juan; GÓMEZ COLOMER, Juan Luis; BARONA VILAR, Silvia; ESPARZA LEIBAR, Iñaki; ETXEBARRIA GURIDI, José Francisco. *Derecho Jurisdiccional III. Proceso Penal.* Valencia: Tirant lo Blanch, 2017, p. 38.

23 Roj: STS 1582/2017 - ECLI: ES:TS:2017:1582.

24 ROJ: STS 1594/2017 - ECLI:ES:TS:2017:1594.

25 ROJ: STS 5362/2015 - ECLI:ES:TS:2015:5362.

26 Así mismo, una recopilación de las sentencias más recientes de la Sala de lo Penal del TS que asientan la doctrina jurisprudencial de los medios de prueba tecnológicos la realizan VILLEGAS GARCÍA, María Ángeles y ENCINAR DEL POZO, Miguel Ángel. Validez de medios de prueba tecnológicos. *Diario La Ley*. Madrid, n. 9005, Sección dossier, 2017.

27 Dispone así el artículo 588 bis a. LECr: "1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

electrónicos (Capítulo VI) y Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (Capítulo VII).[28]

La utilización habitual de las nuevas tecnologías hace necesaria la obtención de prueba de tipo tecnológico que, si bien es cierto que contribuirá a incrementar la eficacia judicial en la persecución de los delitos en igual medida aumentará el riesgo de lesividad del derecho fundamental a la autodeterminación informativa de las personas investigadas. A pesar de la protección constitucional de este derecho fundamental contenido en el art. 18.4 no se ha aprovechado la reforma de la legislación procesal para haber realizado una protección específica del derecho a la protección de los datos personales que pudiera verse con afectado con motivo de la obtención de prueba tecnológica. La importancia de esta protección va a hacer necesario que se legisle en el futuro en el sentido de una protección

---

[28] Existen otro tipo de medidas distintas a las procesales para averiguación del delito y la persona del delincuente. Son medidas de tipo predelictual utilizadas por el Estado a través de los agentes de la autoridad con la finalidad de garantizar la seguridad general que también contienen datos personales y, por lo tanto, necesitadas de la protección que se otorga a los datos de carácter personal. Son medidas policiales como la utilización de videocámaras en lugares públicos regulados por LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (BOE núm. 186, de 5 de agosto de 1997), conservación de datos personales provenientes de comunicaciones electrónicas dispuesto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE núm. 251, de 19/10/2007) y la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (DOUE núm. 119, de 4 de mayo de 2016). Los ficheros policiales utilizados para el ejercicio de la actividad policial que incorporan una ingente cantidad de datos personales y, de especial relevancia, por el tipo de datos personales que se contienen son las bases de datos policiales sobre identificadores de ADN. Los ficheros policiales se rigen por la normativa general de protección de datos personales. Sobre el tratamiento jurídico de los datos de carácter personal en determinadas diligencias de investigación véase al autor ETXEBERRIA GURIDI, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal*, op. cit., pp. 159 y ss. En los casos de delincuencia transfronteriza se deben tener en cuenta las bases de datos de las siguientes instituciones: EUROPOL, EUROJUST y OlAF.

específica de manera separada al resto de derechos fundamentales que se contienen en el art. 18 CE.

3.2. Los dispositivos de almacenamiento masivo de información

El registro de dispositivos de almacenamiento masivo de la información se aborda en los arts. 588 bis sexies a, b y c LECr[29] (Capítulo VIII del Título VIII, Libro II, "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución"). La regulación del registro de los dispositivos de almacenamiento masivo de información refuerza la seguridad jurídica que se necesitaba en la obtención de la prueba electrónica a través de esta diligencia de investigación[30]. Se sigue la doctrina del TS que se incorpora a la

[29] Artículo 588 sexies a. Necesidad de motivación individualizada. Artículo 588 sexies b. Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado. Artículo 588 sexies c. Autorización judicial.

[30] La doctrina ponía así de relieve la necesidad de una autorización judicial expresa habilitante para poder llevar a cabo el registro de este tipo de dispositivos de almacenamiento masivo de la información. Véase entre otros, CASTILLEJO MANZANARES, Raquel, Medios Probatorios, *Hacia un nuevo proceso penal*, op. cit., "...el procedimiento adecuado en estos supuestos, esto es, cuando se trate de la inspección o recogida de dispositivos y soportes de almacenamiento masivo de datos, es que la autorización judicial debería contener expresamente su práctica y sobre qué soportes se ha de realizar". Sobre este tema podemos ver también DELGADO MARTÍN, Joaquín. La prueba electrónica en el proceso penal. *Diario La Ley,* Madrid, n. 8167, Sección Doctrina, 2013; GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. Garantías constitucionales en la persecución penal en el entorno digital. In GONZÁLEZ-CUÉLLAR SERRANO, Nicolás (ccord.). *Derecho y justicia penal en el siglo XXI*: *liber amicorum en homenaje al profesor Antonio González-Cuéllar García*. Madrid: Colex,, 2006, pp. 887-916, pp. 887-916; ORTIZ PRADILLO, Juan Carlos. Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito*. In: PÉREZ GIL, Julio (coord.). Madrid: La Ley, 2012, pp. 267-310; PÉREZ GIL, Julio y GONZÁLEZ LÓPEZ, Juan José. La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal. *Diario La Ley. Madrid,* n. 8217, 2013; CABEZUDO RODRÍGUEZ, Nicolás. Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal. In: JIMENO BULNES, Mar y PÉREZ GIL, Julio (coords.).

regulación; así, entre otras muchas, la sentencia del TS 785/2008, de 25 de noviembre, F. J. 4, recuerda la doctrina consolidada de la Sala[31] "...esta Sala Segunda SSTS 985/2009 de 13.12, 342/2013 de 17.4, 587/2014 de 18.7, tiene declarado que: El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Por lo tanto, la jurisprudencia argumentaba y en esa línea se legisla que los dispositivos de almacenamiento masivo son algo más que una pieza de convicción a aportar a los autos y que habrá que estar a su contenido, ie., se debe tener en cuenta, en lo que en este trabajo concierne, que contiene datos de carácter personal; y en atención a ello es necesario o bien, el consentimiento del titular o un título habilitante, resolución judicial en forma de Auto, que fije, expresamente, los términos y alcance de los dispositivos que deben ser registrados.

3.3 Protección del derecho al entorno virtual

La cantidad y la calidad de información que contienen los dispositivos de almacenamiento masivo hace que resulten implicados diferentes derechos fundamentales. Estos dispositivos pueden contener información, datos sobre la vida personal y profesional de su titular pero, además, conversaciones o comunicaciones con otras personas. Así, estarían afectados el derecho a la intimidad o a la vida privada

Nuevos horizontes del derecho procesal: libro-homenaje al Prof. Ernesto Pedraz Peñalva. Barcelona: Bosch, 2016 . P. 541-558.

31 Roj: STS 7179/2008 - ECLI: ES:TS:2008:7179.

y el derecho al secreto de las comunicaciones junto con el derecho a la protección de los datos personales. El TC ha intentado describir el contenido de cada derecho fundamental atendiendo a los datos individualmente considerados[32] pero esta tarea cede ante el cúmulo de datos contenidos en los dispositivos de almacenamiento que hace que resulte imposible identificar de manera aislada los derechos fundamentales implicados, pues, muchas veces, aparecen entremezclados. El tratamiento individualizado de los datos personales que contienen los dispositivos de almacenamiento de información provoca cierta inseguridad jurídica al no existir una línea jurisprudencial uniforme sobre el contenido y límites del derecho fundamental afectado. Es más, incluso los datos personales tomados en cuenta de manera individualizada o aislada podrían resultar irrelevantes para su tutela jurisdiccional pero su tratamiento conjunto les otorga la necesidad de especial protección al resultar afectada la propia personalidad individual[33].

Se habla entonces del "derecho a la protección del propio entorno virtual". Ya desde la sentencia del TS 342/2013, de 17 de abril, F. J. 8, se pone de manifiesto esta circunstancia y la necesidad de autorización judicial habilitante que justifique el sacrificio del titular del dispositivo a

---

[32] El TC ha ido señalando, de manera casuística, los datos referidos a la vida íntima de la persona individualmente considerados, afirmando que "...el derecho a la intimidad comprende la información relativa a la salud física y psíquica de las personas, quedando afectado en aquellos casos en los que sin consentimiento del paciente se accede a datos relativos a su salud o a informes relativos a la misma" (SSTC 70/2009, Sala 1ª, de 23/03/2009, y 159/2009, Sala 2ª, de 29/06/2009), así como los datos económicos contenidos en el Impuesto de la Renta sobre las Personas Físicas (IRPF) en, entre otras, STC 233/1999, Pleno, de 16/12/1999.

[33] Es significativa en este sentido la sentencia del TC 173/2011, de 7 de noviembre, último párrafo del FJ 3º, que explica la especial idiosincrasia de los datos personales y la forma en que deben tutelarse: "Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona."

la protección de sus datos personales[34]. La importancia de esta sentencia 342/2013 radica, además, en que recoge el tratamiento jurídico que el TS realiza del contenido almacenado en el dispositivo electrónico[35]. Se

[34] Roj: STS 2222/2013 - ECLI: ES:TS: 2013:2222. En el F. J. 8 de la STS 342/2013 se recoge: "El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar -de hecho, normalmente albergará- información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones.

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policia, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal."

[35] El F. J. 8 de la STS342/2013 dice así: "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento

decanta por la protección de "derecho al propio entorno virtual" que lo define como "toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Se trata de contemplar "de forma unitaria" mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado". El TS considera que el tratamiento jurídico de forma unitaria puede ser más adecuado para su protección jurisdiccional y lo denomina "derecho al propio entorno virtual" que tiene un plus de protección superior en el momento de su sacrificio que el tratamiento constitucional individualizado cada uno de esos derechos contemplados en el art. 18 CE.

De esta manera, el TS en la significativa sentencia 489/2018, de 23 de octubre, avala la técnica legislativa empleada en la reforma operada por la LO 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, que

constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital. Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, 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."

comprende de forma unitaria, otorgando el mismo tratamiento jurídico, a todos los datos contenidos en los sistemas de almacenamiento masivo de la información. Es, precisamente, el tratamiento que se haga de los datos el que puede fácilmente describir un perfil personal del titular que es necesario proteger[36]. En palabras de la mencionada sentencia TS 489/2018, F. J. 5: "Algunos precedentes alientan la aparición de un derecho... con cierta vocación de emanciparse para cobrar autonomía e identidad propias. Partiendo de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (*smartphone*) se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un derecho al entorno digital. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional (SSTS 342/2013, de 17 de abril; 587/2014, de 24 de febrero, y 587/2014, de 18 de julio).

De ahí que en nuestra renovada legislación procesal haya emergido en fechas recientes, como diligencia específica que reclama garantías singulares (diferentes al registro de un vehículo o una maleta, por ejemplo), el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a) LECrim y ss., introducidos por la LO 13/2015, de 5 de octubre)." "...el mandato va dirigido a las fuerzas policiales... Pero ayuda la referencia en cuanto que, en buena medida, tal legislación se limita a conferir formato normativo a ideas ya presentes y exigidas en jurisprudencia precedente." Por lo tanto, la valoración por el juez de la procedencia de la medida de investigación del registro de dispositivos de almacenamiento masivo de información (debemos entender incluidos los equipos o sistemas informáticos) no requerirá la necesidad de precisar el derecho fundamental concretamente vulnerado sino tendrá como objetivo la protección del entorno virtual[37]. Y sólo en

---

[36] DELGADO MARTÍN, Joaquín. Derechos Fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos. *Diario La Ley*. Madrid, n. 8202, 2013. P. 3.

[37] En este sentido se pronuncia la sentencia del TS 342/2013, 17 de abril de 2013, F.J. 8 A) cuando argumenta que "La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de

el examen posterior, a la hora de motivar la adopción de la medida se entrará en el análisis particular de los derechos controvertidos.[38]

3.4 Extensión y límites del registro de dispositivos de almacenamiento masivo de la información

La necesidad de autorización judicial para acceder al contenido de los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, que se incauten con independencia de un registro domiciliario se exige en el art. 588 sexies c. LECr[39]. Y el contenido de la resolución judicial que autorice la medida deberá ser el que se establece en el punto 3 del art. 588 bis c[40]. Además de los requisitos referidos al hecho punible, la identidad de los investigados y la duración de la medida, entre otros, este artículo contiene la extensión y los límites en los que

---

vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos.".

[38] De esta manera lo argumenta la Circular de la Fiscalía General del Estado 5/2019, sobre registro de dispositivos y equipos informáticos, p. 7. Disponible en: <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_5-2019.pdf?idFile=2a2c765e-3a04-4656-87c0-8b56ef73d0b6 >. Acceso en: 22 de junio de 2019.

[39] Se trata de las disposiciones comunes a las medidas de investigación tecnológica que se recogen el el Capítulo IV del Título VIII LECr: interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

[40] Vemos el contenido expreso en el punto 3 del art. 588 bis c. LECr.

se tiene que desarrollar esta medida de investigación tecnológica. De esta manera, el Auto que acuerde la medida de investigación debe determinar la extensión de la medida de injerencia, especificando su alcance, así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a LECr[41]. Se trata de especificar en la resolución judicial los términos exactos del registro, ie., los instrumentos o dispositivos tecnológicos a investigar, si en el mismo registro se podrá hacer copias de los datos que contengan los dispositivos, las condiciones para proteger la integridad de los datos que se aprehendan y establecer las garantías necesarias en el caso de un posterior análisis pericial[42].

El alcance del registro debe venir referido a la clase información o datos a los que se podrá acceder a través de la habilitación judicial que se deberá detallar, sin que exista necesidad de precisar los soportes físicos o virtuales que los contengan y que se puedan localizar con motivo del registro habida cuenta de la imposibilidad de enumerar todos los sistemas que los puedan contener dada su diversidad, por lo que bastará que el mandamiento judicial realice una mención genérica. De esta manera, se puede concretar el registro de los dispositivos de almacenamiento masivo a los datos referidos a la persona investigada con irrelevancia de la pertenencia del mismo incluso cabe la posibilidad que se habilite a registrar los datos almacenados con independencia de su titularidad. Se puede también especificar el tipo de información a la que se puede acceder, ie., a la clase de datos a que se registrarán teniendo en cuenta la tipología de datos existentes [43]. La posibilidad de acotar con precisión la medida de investigación de los dispositivos

---

[41] Recordaremos que estos principios de idoneidad, excepcionalidad, necesidad y proporcionalidad son doctrina reiterada del TC y se incorporan a la LECr mediante su reforma por LO 13/2015Cr.

[42] Sobre los términos en los que se tiene que desarrollar el registro de estos aparatos podemos consultar FERNÁNDEZ-GALLARDO,Javier Ángel. Registro de dispositivos de almacenamiento masivo de la información.-, *Revista jurídica de la Universidad de Santiago de Compostela,* vol. 25, n. 2, 2016, pp. 40-41.

[43] Se posibilita, por tanto, un registro selectivo como indica CABEZUDO RODRÍGUEZ, Nicolás. Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *I*

de almacenamiento masivo de información supondrá respetar los principios de excepcionalidad y necesidad que rigen este tipo de intervenciones pero no siempre y en todos los casos se estará en disposición de realizar un detalle tan preciso de la medida de investigación que se habilita realizar y, en este caso, habrá que valorar si se trata de una mera infracción procesal o si, por el contrario, se produce una situación de indefensión en el que se ha visto vulnerado el derecho de defensa[44] .

3.5. Acceso a los datos por la Policía Judicial y consentimiento del interesado

La posibilidad de acceso a los datos personales contenidos en dispositivos de almacenamiento masivo de la información sin autorización judicial es posible en dos supuestos: se trata de los casos de urgencia o en el caso de consentimiento del interesado. Son supuestos en los que el monopolio jurisdiccional cede ante la necesidad de autorización judicial para acceder a los datos personales[45]. El primero de ellos, son actuaciones que lleve a cabo la Policía Judicial en los casos

Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal" de 5 de noviembre de 2015.-, Madrid: Ministerio de Justicia, 2016, pp. 7-60

[44] Recordemos la jurisprudencia consolidada sobre la vulneración formal o la vulneración material de las normas procesales a los efectos que se pueda tutelar la existencia de una indefensión con relevancia constitucional: Sentencia TC 25/2011, de 14 de marzo (BOE núm. 86, de 11 de abril de 2011) ECLI:ES:TC:2011:25 y Sentencia TC 82/2002, de 22 de abril (BOE núm. 122, de 22 de mayo de 2002) ECLI:ES:TC:2002:82, entre muchas otras.

[45] FERNÁNDEZ-GALLARDO, Javier Ángel, Registro de dispositivos de almacenamiento masivo de la información, op. cit., pp. 48-51 recuerda que es doctrina consolidada del TC que la afectación de un derecho fundamental no es suficiente para justificar como presupuesto indispensable la previa autorización judicial salvo explícita habilitación legal; recuerda, por ejemplo, el registro de una maleta o de unos papeles que realiza la Policía sin necesidad de expresa autorización judicial. Así recoge: "La incidencia en la privacidad no lleva a cuestionar que pueda recibirse declaración a un testigo por la policía como medio de averiguación del delito, sin necesidad de previa autorización judicial motivada, ni de ningún otro requisito especial. Ni siquiera cuando ese interrogatorio, por exigencias de la investigación, conduce a adentrarse en reductos más sensibles de la privacidad"

de urgencia. Esta situación se regula por el apartado cuarto del art. 588 sexies c LECr en el que se recoge el supuesto de acceso directamente por la Policía Judicial a los datos que contenga el dispositivo incautado sin necesidad de autorización judicial previa. Se trata de los casos de urgencia en los que se aprecie un interés constitucional legítimo y que sea imprescindible la medida. En estos asuntos la Policía Judicial debe comunicar al Juez de manera inmediata y, en todo caso, en el plazo máximo de 24 horas, la actuación que se ha llevado a cabo para que el Juez competente, de forma motivada, revoque o confirme la actuación en un plazo máximo de 72 horas desde que la Policía Judicial ordenó la medida.

Esta posibilidad que ahora contempla la LECr estaba avalada por la doctrina constitucional; así, la sentencia TC 70/2002 reconoce, "La regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, 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. Esa 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 esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad."[46]Se establece el requisito temporal como motivo habilitante de la actuación judicial que supone que su transcurso puede perjudicar la investigación penal. En definitiva, se trata de proteger el interés general del Estado de persecución de los delitos por encima del derecho a la protección de los datos. Vemos aquí la aplicación de una dimensión de esa limitación del derecho fundamental a la protección de los datos personales que comentamos en epígrafe anterior.

[46] Se trata del FJ 9 de la Sentencia 70/2002, de 3 de abril (BOE núm. 99, de 25 de abril de 2002) ECLI:ES:TC:2002:70.

La siguiente exclusión, que señalábamos, a la necesidad de autorización judicial para el acceso a los datos contenidos en los dispositivos de almacenamiento masivo de la información es la referida a la prestación del consentimiento por el interesado. La exigencia del consentimiento únicamente se exige en el grado de tácito sin necesidad de que el titular del dispositivo debe realizar un consentimiento expreso. Si bien, la LECr guarda silencio sobre este aspecto del consentimiento pues no lo regula, el TC se ha pronunciado sobre el mismo en el aspecto indicado siendo relevante, entre otras la sentencia del TC 173/2011 que ampara el acceso a datos personales contenidos en dispositivos electrónicos a través de un consentimiento tácito del titular del mismo valorando también la extensión del consentimiento otorgado, ie., que la actuación invasiva de los datos no se haya extralimitado[47]. En cualquier caso, pese al esfuerzo del TC por amparar el consentimiento para el acceso de datos personales contenidos en los dispositivos de almacenamiento masivo se echa de menos en la tan reciente regulación de las medidas de investigación tecnológicas, recordemos por LO 13/2015, una regulación de las condiciones en las que se debe prestar ese consentimiento ya establecidas.

[47] La Sentencia 173/2011, de 7 de noviembre (BOE núm. 294, de 07 de diciembre de 2011). ECLI:ES:TC:2011:173 es clave en este tema que recoge el parecer del Alto Tribunal, así su FJ 2; "...hemos afirmado que el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto "aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2). En lo relativo a la forma de prestación del consentimiento, hemos manifestado que éste no precisa ser expreso, admitiéndose también un consentimiento tácito. Así, en la STC 196/2004, de 15 de noviembre, en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconocimos no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9)".

Conclusiones: Efectos de la prueba obtenida mediante registro de dispositivos de almacenamiento masivo de la información vulnerando el derecho fundamental a la protección de los datos de carácter personal

Si partimos de la alta protección que se otorga a los datos de carácter personal como derecho fundamental hemos de llegar a la conclusión que la obtención de prueba vulnerando este derecho especialmente protegido debe tener unas consecuencias perjudiciales en su valoración. La más perjudicial sería la ilicitud de la prueba. A pesar de esta afirmación, no existe aún pronunciamiento jurisprudencial claro al respecto habida cuenta de que apenas hay alegaciones sobre la vulneración de ese derecho. Pero es que, además, en las pocas sentencias en que se trata la vulneración de los datos de carácter personal y su posible ilicitud a efectos probatorios se contempla de forma unitaria independientemente del formato en que se encuentren y se opta por una protección genérica: la protección del "derecho al entorno virtual o digital". Relevante en este tema es la sentencia del TS 287/2017 [48], que desestima el motivo de impugnación (F. J. 2, 2.1): "Mal puede hablarse, por tanto, de vulneración del derecho a la intimidad o al entorno virtual del acusado cuando los peritos no pudieron acceder a ningún contenido susceptible de ser protegido por su conexión con aquellos derechos. Bastaría, por tanto, subrayar que ningún dato privado del acusado llegó a incorporarse a la causa, a raíz del análisis del ordenador, para descartar la reivindicada alegación de prueba ilícita".

Tampoco reciben el mismo tratamiento jurisprudencial los datos de carácter personal que se han obtenido por un particular que los aprehendidos por la policía judicial con motivo de una investigación penal. Así, la sentencia del TS 116/2017, de 23 de febrero[49] que en el F. J. 6, distingue los dos supuestos: "...está fuera de discusión la necesidad

[48] Roj: STS 1487/2017 - ECLI: ES:TS:2017:1487. En este caso se desestima el motivo de impugnación (F. J. 2, 2.1): "Mal puede hablarse, por tanto, de vulneración del derecho a la intimidad o al entorno virtual del acusado cuando los peritos no pudieron acceder a ningún contenido susceptible de ser protegido por su conexión con aquellos derechos. Bastaría, por tanto, subrayar que ningún dato privado del acusado llegó a incorporarse a la causa, a raíz del análisis del ordenador, para descartar la reivindicada alegación de prueba ilícita."

[49] Roj: STS 471/2017 - ECLI: ES:TS:

de excluir el valor probatorio de aquellas diligencias que vulneren el mandato prohibitivo del art. 11 de la LOPJ. Pero más allá del fecundo debate dogmático acerca de lo que se ha llamado la eficacia horizontal de los derechos fundamentales, es evidente que la acción vulneradora del agente de la autoridad que personifica el interés del Estado en el castigo de las infracciones criminales nunca puede ser artificialmente equiparada a la acción del particular que, sin vinculación alguna con el ejercicio del ius puniendi, se hace con documentos que, más tarde, se convierten en fuentes de prueba que llegan a resultar, por una u otra circunstancia, determinantes para la formulación del juicio de autoría. El particular que por propia iniciativa desborda el marco jurídico que define la legitimidad del acceso a datos bancarios, ya actúe con el propósito de lograr un provecho económico, ya con el de fomentar el debate sobre los límites del secreto bancario, no lo hace en nombre del Estado. No rebasa el cuadro de garantías que define los límites constitucionales al acopio estatal de fuentes de pruebas incriminatorias. Nada tiene que ver esa actuación con la de un agente al servicio del Estado. Lo que proscribe el art. 11 de la LOPJ no es otra cosa que la obtención de pruebas (" no surtirán efecto las pruebas obtenidas...."). Es el desarrollo de la actividad probatoria en el marco de un proceso penal - entendido éste en su acepción más flexible- lo que queda afectado por la regla de exclusión cuando se erosiona el contenido material de derechos o libertades fundamentales". Del contenido de la sentencia se extrae que la consecuencia de la ilicitud de la prueba vulnerando un derecho fundamental, en este caso el de la protección de los datos personales, está dirigida a la actuación de los agentes de la autoridad para hacer efectivo el *ius puniendi* del Estado.

Incluso en alguna sentencia anterior, sentencia del TS 949/2006, de 4 de octubre de 2006[50] se concibe la vulneración del derecho a la autodeterminación informativa como conculcación de la normativa general de protección de datos de carácter general y no como ilicitud de la prueba por vulneración de derechos fundamentales en su obtención. En el F. J. 1 se recoge: "...si el almacenamiento de datos excesivos o innecesarios perjudica o contravine la normativa de la Ley de Protección

[50] Roj: STS 6190/2006 - ECLI: ES:TS:2006:6190.

de Datos será competencia de la Agencia de Protección de Datos investigar el fichero y reducirlo a los términos previstos por la Ley, pero todo ello para nada afecta a la identificación previa realizada con criterios adecuados. Es más, la Orden de 2.9.2003 del Departamento de Interior Vasco, limita su finalidad a las actividades de policía científica orientadas a relacionar personas con el espacio físico de la infracción penal. En atención a lo expuesto resulta que cualquier temor o recelo de un potencial ataque al "habeas data" está injustificado, sin que por otro lado tales temores tengan que ver con la vulneración del derecho fundamental a la intimidad de la recogida y custodia de muestras si tal cometido se ha realizado con plena acomodación a la normativa vigente. Lo que nunca puede excluirse -recuerda la sentencia citada 179/2006 de 14.2- es que cualquier persona pueda infringir la Ley, en cuyo caso estaría sujeto a las correspondientes sanciones penales o disciplinarias que fueran pertinentes. Pero esa eventualidad en nada afecta a la prueba practicada y a la recogida y conservación de las muestras genéticas, que en ningún aspecto atacan al derecho fundamental contemplado en el art. 18.1 CE.

En relación a la vulneración del art. 18.4 CE que consagra el derecho a la autodeterminación informativa, derecho que debe entenderse como aquel que ostenta toda persona física a la reserva y control de los datos que le conciernen en los distintos ámbitos de la vida, de tal suerte que pueda decidir en todo momento cuando, como y en qué medida esa información sea recogida, almacenada, tratada y en su caso transferida a terceros, así como a ser informado de los datos personales que a estos efectos se encuentren almacenados en ficheros o bases de datos, pudiendo acudir a los mismos con la posibilidad de exigir su identificación, puesta al día o cancelación . No obstante, este derecho como todos, tiene excepciones y puede ser limitado por razones de otro interés preponderante. En la Ley de Protección de datos se establece en el art. 6 la exigencia del consentimiento inequívoco del afectado, pero en el mismo precepto se establecen excepciones" (...) " Y en todo caso -insistimos- el hipotético incumplimiento del registro constituirá una irregularidad administrativa que en modo alguno supone la vulneración de un derecho fundamental que lleve aparejada la nulidad absoluta del análisis practicado".

Lo cierto es que no existe una distinción clara respecto a la normativa que es necesario aplicar en estos supuestos. Se ha superado la regulación incompleta y obsoleta que venía establecida por el Reglamento 1/2005, de aspectos accesorios a las actuaciones judiciales, aprobado por Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial y por la LOPJ, art. 230.5 LOPJ por una más amplia y específica regulada en la legislación orgánica, mediante la LOPJ en su última modificación efectuada por la Ley Orgánica 7/2015, de 21 de julio añade por el art. único 36 el Capítulo I bis, el art. 236 bis al decies, sobre la Protección de datos de carácter personal en el ámbito de la Administración de Justicia. Pero se constata una deficiente cobertura legal en el ámbito jurisdiccional que, en ocasiones, se confunde con la normativa general de protección de los datos personales regulada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales lo que ocasionará más de un problema en la práctica jurídica respecto a la normativa a aplicar. Se debería haber apostado por una regulación procesal específica dentro de la LECr y no en la legislación orgánica que regulara el tratamiento de los datos personales que se realiza en el ámbito jurisdiccional y los efectos que en el proceso penal provoca la obtención de la prueba vulnerando el derecho a la protección de los datos personales.

Conviene poner de manifiesto las consecuencias que en el proceso penal debe tener la obtención de manera ilícita de datos personales del investigado a los efectos de la valoración de la prueba así como, cuestionarse las consecuencias jurídicas del tratamiento ilegal de datos personales del imputado "obtenidos con motivo de una investigación penal anterior e incluidos en una base de datos para su utilización en otros procesos penales"[51]. Incluso, cuestionarse el tratamiento jurisdiccional que se otorga a los datos personales en "... el período que transcurre entre la obtención y la celebración del juicio

[51] Así lo cuestiona GUTIÉRREZ ZARZA, María Ángeles. La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?. *La Ley penal*, Madrid, n. 71, 2010, p. 4 que entiende que la protección de los datos personales debe formar parte del conjunto de principios y derechos del proceso penal.

oral"[52]. Será necesario garantizar la integridad de los datos durante la tramitación del proceso penal[53].

Queda, aún, avanzar en el estudio de las consecuencias procesales que se derivan de la obtención de datos obtenidos de manera ilícita en los dispositivos de almacenamiento masivo que es la fuente de prueba que hemos analizado en este trabajo. Entiendo hubiera sido necesario que la reciente reforma de la legislación procesal penal realizase una protección específica del derecho a la protección de los datos personales afectado con motivo de la obtención de prueba tecnológica[54]. La importancia de los datos personales, que irá en aumento, se traducirá en otorgar mayores garantías procesales; lo cual hará necesario que se legisle en el sentido de una protección específica de manera separada al resto de derechos fundamentales que se contienen en el art. 18 CE. La normativa procesal

---

[52] ESPARZA LEIBAR, Iñaki. Protección de datos de carácter personal y proceso penal *El nuevo proceso penal sin código procesal penal*, celebrado en la Universidad de Santiago de Compostela, los días 9 y 10 de noviembre de 2017. In: ORDEÑANA GEZURAGA, Ixusko (coord.). *Justicia con ojos de mujer. Cuestiones procesales controvertidas.* Valencia: Tirant lo Blanch, 2018.

[53] DELGADO MARTÍN, Joaquín. Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley,* Madrid, n. 8693, Sección doctrina, 2016, p. 3, destaca el problema de la manipulación de los datos: "...los datos pueden ser fácilmente modificados, sobre-escritos o borrados, lo que determina un peligro evidente de manipulación de las pruebas. De esta forma resulta necesario utilizar técnicas que permitan obtener dichos datos y garantizar su autenticidad e integridad durante la tramitación del proceso (cadena de custodia)." Las consecuencias en el proceso penal de los datos personales obtenidos violentando este derecho fundamental también lo pone de relieve FRÍAS MARTÍNEZ, Emilio. Protección y tratamiento de datos personales por el Ministerio Fiscal. *La Ley penal,* Madrid, n. 71, 2010. Protección de datos en el proceso penal, p. 7, quien no duda de la ilicitud de la prueba así obtenida: "Al elevar la protección de los datos de carácter personal a la categoría de derecho fundamental, la ilicitud en la obtención de los mismos tendrá consecuencias directas en la consideración de su valor probatorio, pues indudablemente los datos que hayan sido obtenidos con quebranto del derecho fundamental no podrán ser valorados para desvirtuar la presunción de inocencia".

[54] La doctrina procesal coincide en esta idea; así LÓPEZ-BARAJAS PEREA, Inmaculada. Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos, *Revista de Internet, Derecho y Política.* Madrid, n. 24, 2017, p. 73, p. 73, señala, también, alguna de las deficiencias normativas apuntadas.

deberá desarrollarse con mayor amplitud para dar mejor cobertura legal a los datos de carácter personal del investigado o encausado en el proceso penal.

No existe en este tema aún pronunciamiento jurisprudencial claro sobre las consecuencias de la valoración de la prueba vulnerando este derecho de protección de datos de carácter personal. No son muchas tampoco las alegaciones de parte sobre la ilicitud de la prueba con motivos de la vulneración de este derecho, quizá por esa falta de conciencia general sobre la protección de los datos personales a la que al principio del trabajo aludíamos. Pero es que, además, en las pocas sentencias en que se trata la vulneración de los datos de carácter personal y su posible ilicitud a efectos probatorios se contempla de manera conjunta junto con el resto de derechos fundamentales contenidos en el art. 18 CE y se opta por la protección del "derecho al entorno virtual o digital" al considerarlo con un plus de protección mayor que si se aprecian de manera individual . En cualquier caso, el acceso, a efectos probatorios, de los datos personales en el entorno virtual, que revelan el perfil personal del investigado, se ha de convertir en uno de los retos futuros que el legislador deberá plantearse proteger desde el ámbito de las garantías procesales[55].

Referencias bibliográficas

BANACLOCHE PALAO, Julio; ZARZALEJOS NIETO, Jesús. Las diligencias de investigación restrictivas de los derechos fundamentales. In: *Aspectos fundamentales del Derecho Procesal Penal*. Madrid: La Ley, 3ª ed., 2015.

BARONA VILAR, Silvia. La prueba (I). In: MONTERO AROCA, Juan; GÓMEZ COLOMER, Juan Luis; BARONA VILAR, Silvia; ESPARZA LEIBAR, Iñaki; ETXEBARRIA GURIDI, José Francisco. *Derecho Jurisdiccional III. Proceso Penal*. Valencia: Tirant lo Blanch, 2017.P. 38

[55] Recordemos, como arriba hemos apuntado, la falta de regulación en la LECr de las condiciones en las que el investigado debe prestar su consentimiento para poder acceder a su entorno virtual para que tenga validez en el proceso. Podemos ver un estudio de esta problemática realizado por FERNÁNDEZ-GALLARDO, Javier Ángel. El consentimiento del detenido al acceso a sus redes sociales y dispositivos de almacenamiento masivo de información. *La Ley Penal,* Madrid, n. 126, Sección Legislación aplicada a la práctica, 2017.

CABEZUDO RODRÍGUEZ, Nicolás. Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal. In:JIMENO BULNES, Mar y PÉREZ GIL, Julio (coords.). *Nuevos horizontes del derecho procesal: libro-homenaje al Prof. Ernesto Pedraz Peñalva.)* Barcelona: Bosch, 2016 . P. 541-558.

CABEZUDO RODRÍGUEZ, Nicolás. Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal. *I Jornada del Boletín del Ministerio de Justicia: Las reformas del proceso penal"* de 5 de noviembre de 2015.-, Madrid: Ministerio de Justicia, 2016. P. 7-60.

CASTILLEJO MANZANARES, Raquel.-, Hacia un nuevo proceso penal. Madrid: La Ley,, 2010.

CIRCULAR de la Fiscalía General del Estado 5/2019, sobre registro de dispositivos y equipos informáticos, p. 7. Disponible en: <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Circular_5-2019.pdf?idFile=2a2c765e-3a04-4656-87c0-8b56ef73d0b6>. Acceso en: 22 de junio de 2019.

DELGADO MARTÍN, Joaquín. Derechos Fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos. *Diario La Ley*.-Madrid, n. 8202, p. 3.

DELGADO MARTÍN, Joaquín. Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley,* Madrid, n. 8693, Sección doctrina, 2016, p. 3.

DELGADO MARTÍN, Joaquín. La prueba electrónica en el proceso penal. *Diario La Ley,* Madrid, n. 8167, Sección Doctrina, 2013.

ESPARZA LEIBAR, Iñaki. Protección de datos de carácter personal y proceso penal *El nuevo proceso penal sin código procesal penal*, celebrado en la Universidad de Santiago de Compostela, los días 9 y 10 de noviembre de 2017. In: ORDEÑANA GEZURAGA, Ixusko (coord.). *Justicia con ojos de mujer. Cuestiones procesales controvertidas.* Valencia: Tirant lo Blanch, 2018.

ETXEBERRIA GURIDI, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal.* Madrid: Agencia de protección de Datos, Premio Protección de datos Personales,, 1998, pp. 22 y 159 y ss.

FERNÁNDEZ-GALLARDO, Javier Ángel. El consentimiento del detenido al acceso a sus redes sociales y dispositivos de almacenamiento masivo de información. *La Ley Penal,* Madrid, n. 126, Sección Legislación aplicada a la práctica, 2017.

FERNÁNDEZ-GALLARDO,Javier Ángel. Registro de dispositivos de almacenamiento masivo de la información.-, *Revista jurídica de la Universidad de Santiago de Compostela,* vol. 25, n. 2, 2016, pp. 40-41.

FRÍAS MARTÍNEZ, Emilio. Protección y tratamiento de datos personales por el Ministerio Fiscal. *La Ley penal,* Madrid, n. 71, 2010. Protección de datos en el proceso penal, p. 7.

GONZÁLEZ-CUÉLLAR SERRANO, Nicolás. Garantías constitucionales en la persecución penal en el entorno digital.In GONZÁLEZ-CUÉLLAR SERRANO, Nicolás (ccord.). *Derecho y justicia penal en el siglo XXI*: *liber amicorum en homenaje al profesor Antonio González-Cuéllar García.* Madrid: Colex,, 2006, pp. 887-916.

GUTIÉRREZ ZARZA, María Ángeles. La protección de datos personales como derecho fundamental del imputado, ¿también en el ámbito del proceso penal?. *La Ley penal*, Madrid, n. 71, 2010, p. 4.

GUTIÉRREZ ZARZA, María Ángeles.-, Protección de Datos Personales en la Carta de Derechos Fundamentales de la Unión Europea y El Tratado de Funcionamiento de la Unión Europea. In: GUTIÉRREZ ZARZA, María Ángeles (coord.). *Nuevas Tecnologías, Protección de Datos Personales y Proceso Penal.* Madrid: La Ley,, 2012.

LÓPEZ-BARAJAS PEREA, Inmaculada. Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos, *Revista de Internet, Derecho y Política.* Madrid, n. 24, 2017, p. 73.

MARCOS AYJÓN, Miguel. Las múltiples implicaciones de la protección de datos en la justicia penal. In: GUTIÉRREZ ZARZA, María Ángeles(coord.). *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017: II Anuario ReDPE.*), Madrid: Wolters Kluwer, 2018.

MURILLO DE LA CUEVA, Pablo Lucas. La Constitución y el derecho a la autodeterminación informativa. *Cuadernos de Derecho Público.* Madrid, n. 19 – 20 2003), pp. 31, 36 – 39.

MURILLO DE LA CUEVA, Pablo Lucas. La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Jurídicos (Nueva época).* Madrid, n. 104, 1999.

ORTIZ PRADILLO, Juan Carlos. Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica. *El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito*. In: PÉREZ GIL, Julio (coord.). Madrid: La Ley, 2012, pp. 267-310.

PÉREZ ESTRADA, M. Josune. Efectos de la vulneración de la protección de los datos personales en el proceso penal. *La Ley Penal*, n. 35, Madrid, 2018.

PÉREZ GIL, Julio y GONZÁLEZ LÓPEZ, Juan José. La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal. *Diario La Ley. Madrid,* n. 8217, 2013.

PÉREZ LUÑO, Antonio Enrique. *Del Habeas Corpus al Habeas Data*. Conferencia impartida en el XIV Curso de Informática y Derecho. Centro Regional de la UNED, Extremadura, 1990, p. 154 – 155.

Disponible en: <http://egov.ufsc.br/portal/sites/default/files/6_16.pdf>. Acceso en: 07de junio de 2018.

PÉREZ LUÑO, Antonio Enrique. Intimidad y protección de datos personales: del „habeas corpus" al „habeas data. In: GARCÍA SAN MIGUEL, Luis (coord.). *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos, 1992, pp. 36 – 45.

PIÑAR MAÑAS, José Luis. La protección de datos personales y ficheros automatizados. In: ROMEO CASABONA, Carlos María (coord.). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares, 2006, pp. 153-167.

SANCHÍS CRESPO, Carolina-., La prueba en soporte electrónico. In: GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián, (coords.). (, *Las tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*. Navarra: Thomson Reuters-Aranzadi,, 2012, p. 713.

VILLEGAS GARCÍA, María Ángeles y ENCINAR DEL POZO, Miguel Ángel. Validez de medios de prueba tecnológicos. *Diario La Ley*. Madrid, n. 9005, Sección dossier, 2017.

Informações adicionais e declarações dos autores
(integridade científica)

Agradecimentos (acknowledgement): Trabajo realizado en el contexto de las actividades que realiza el Grupo de investigación consolidado "Derechos Fundamentales y Unión Europea. Especial referencia al Espacio de Libertad, Seguridad y Justicia de la Unión Europea" (GIC IT-673-13, 2019-2021), financiado por el Gobierno Vasco.

Declaração de conflito de interesses (conflict of interest declaration): o autor confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): o autor assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 05/07/2019
- Controle preliminar e verificação de plágio: 12/07/2019
- Avaliação 1: 23/07/2019
- Avaliação 2: 29/07/2019
- Decisão editorial preliminar: 23/08/2019
- Retorno rodada de correções: 08/09/2019
- Decisão editorial final: 20/09/2019

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editora-associada: 1 (CC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

PÉREZ ESTRADA, Miren J. La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1297-1330, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.253