© **Dereito** Vol.25, nº 2:25-58 (Xullo-Decembro, 2016) • ISSN 1132-9947

REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO DE INFORMACIÓN

Registration of storage devices

DOI: http://dx.doi.org/10.15304/dereito.25.2.3522

JAVIER ÁNGEL FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO
Letrado de la Administración de Justicia
Juzgado Central de Instrucción nº 2 de la Audiencia Nacional
Doctor en derecho
javierangel.fernandez-gallardo@justicia.es

Resumen
Hasta la reforma llevada a cabo por la LO 13/2015 la LECRIM no preveía de una manera expresa la posibilidad de practicar un registro de dispositivos de almacenamiento masivo de información, pese a que la enorme cantidad de información que se acumula en estos dispositivos puede tener un alto interés de cara a esclarecer numerosos hechos delictivos, y olvidando que el acceso a tales contenidos supone una grave intromisión en el derecho a la intimidad, que por tanto debe tener un marco que le dote de certeza y seguridad jurídica, respetando los parámetros de calidad de Ley establecidos en la jurisprudencia del TEDH. En el presente estudio analizaremos los requisitos y garantías que esta nueva regulación exige para el acceso a los datos contenidos en estos dispositivos a efectos de una investigación criminal.
Palabras clave: Intimidad, entorno virtual, ordenador, almacenamiento masivo, volcado.

Abstract
Until the reform carried out by Organic Act 13/2015, the Criminal Procedure Act did not provide an express way the possibility of practicing a record of storage devices, despite the enormous amount of information that accumulates in these devices may have high interest with regard to clarify many crimes. But we cannot forget that access to such content constitutes a serious interference with the right to privacy, which must therefore have a framework that will equip legal certainty and security, respecting the parameters quality of law established in the jurisprudence of the ECHR. In the present study we analyze the requirements and guarantees that this new regulation demands for access to the data contained on these storage devices for the purposes of a criminal investigation.
Keywords: privacy, virtual network, computer, storage devices, dump information.

Recibido: Agosto 2016. Aceptado: Diciembre 2016

1. INTRODUCCIÓN

Conforme a la jurisprudencia del TC[1], el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona, implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana[2]. Entiende dicho Tribunal que el art. 18.1 CE garantiza un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio[3]. Del precepto constitucional citado se deduce que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido[4].

Asimismo el TC[5] manifiesta que la inviolabilidad del domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen

[1] STC 173/2011, Sala 2ª, de 7.11.2011 (BOE núm. 294 de 7.12.2011; MP: Eugeni Gay Montalvo).
[2] SSTC 159/2009, Sala 2ª, de 29.06.2009 (BOE núm. 181 de 28.07.2009; MP: Vicente Conde Martín de Hijas); 206/2007, Sala 1ª, de 24.09.2007 (BOE núm. 261 de 31.10.2007; MP: Manuel Aragón Reyes); 196/2004, Sala 1ª, de 15.11.2004 (BOE núm. 306 de 21.12.2004; MP: Javier Delgado Barrio); y 207/1996, Sala 1ª, de 16.12.1996 (BOE núm. 19 de 22.01.1997; MP: Vicente Gimeno Sendra).
[3] SSTC 89/2006, Sala 1ª, de 27.03.2006 (BOE núm. 106 de 4.05.2006; MP: María Emilia Casas Baamonde); y 127/2003, Sala 2ª, de 30.06.2003 (BOE núm. 181 de 30.07.2003; MP: Pablo Cachón Villar).
[4] STC 70/2009, Sala 1ª, de 23.03.2009 (BOE núm. 102 de 27.04.2009; MP: María Emilia Casas Baamonde).
[5] STC 110/1984, Sala 1ª, de 26.11.1984 (BOE núm. 305 de 21.12.1984; MP: Ángel Latorre Segura).

como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada[6]. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. Estos derechos han adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, orientada a la plena efectividad de estos derechos fundamentales. En efecto, habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos, se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada[7].

En armonía con lo anterior, el TC ha venido describiendo casuísticamente una serie de supuestos, en que, con independencia de las libertades tradicionales antes mencionadas, ha podido sobrevenir una injerencia no admisible en el ámbito de la vida privada e íntima de la persona. En este sentido afirma 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"[8]. Igualmente no hay duda de que, en principio, los datos relativos a la situación económica de una persona entran dentro de la intimidad constitucionalmente protegida[9], que en las declaraciones del IRPF se ponen de manifiesto datos que pertenecen a la intimidad constitucionalmente tutelada de los sujetos pasivos[10], y que la información concerniente al gasto en que incurre un obligado tributario, no sólo forma parte de dicho ámbito, sino que a través de su investigación o indagación puede penetrarse en la zona más estricta de la vida privada o, lo que es lo mismo, en los aspectos más básicos de la autodeterminación personal del

[6] M .T. GERALDES DA CUNHA LOPES, "Derecho a la intimidad y la protección de datos en la era de la seguridad global. Principios constitucionales versus riesgos tecnológicos", en *Anuario Jurídico y Económico Escurialense,* núm. 48, 2015, pp. 6-7.

[7] STC 119/2001, Pleno, de 24.05.2001 (BOE núm. 137 de 8.06.2001; MP: Manuel Jiménez de Parga y Cabrera). A esta nueva realidad ha sido sensible la jurisprudencia del TEDH, como se refleja en las SSTEDH de 21.02.1990 (Series A núm. 172, Powell y Rayner c. Reino Unido); 9.12.1994 (Series A núm. 303-C, López Ostra c. Reino de España); y 19.02.1998 (*Reports of Judgments and Decisions* 1998-I, Guerra y otros c. Italia).

[8] SSTC 70/2009, Sala 1ª, de 23.03.2009, cit.; y 159/2009, Sala 2ª, de 29.06.2009, cit.

[9] STC 233/1999, Pleno, de 1612.1999 (BOE núm. 17 de 20.01.2000; MP: Pablo Cachón Villar).

[10] STC 47/2001, Pleno, de 15.02.2001 (BOE núm. 65 de 16.03.2001; MP: Pedro Cruz Villalón).

individuo[11].

Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido[12], menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. 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[13]. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE, por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación, sino también el derecho a la intimidad personal, reconocido en el art. 18.1 CE , en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático

[11] STC 233/2005, Sala 2ª, de 26.09.2005 (BOE núm. 258 de 28.10.2005; MP: Guillermo Jiménez Sánchez). Por otra parte, la STC 70/2002, Sala 1ª, de 3.04.2002 (BOE núm. 99 de 25.04.2002; MP: Fernando Garrido Falla), en un supuesto en que un guardia civil había intervenido a un detenido una agenda personal y un documento que se encontraba en su interior, sostuvo que "con independencia de la relevancia que ello pudiera tener a los fines de la investigación penal y, por tanto, de su posible justificación, debemos afirmar que la apertura de una agenda, su examen y la lectura de los papeles que se encontraban en su interior supone una intromisión en la esfera privada de la persona a la que tales efectos pertenecen, esto es, en el ámbito protegido por el derecho a la intimidad, tal como nuestra jurisprudencia lo define".

[12] J. DELGADO MARTÍN, "Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos", en *Diario La Ley*, núm. 8202, 29.11. 2013, p. 3.

[13] A la misma conclusión llega la STC 230/2007, Sala 1ª, de 5.11.2007 (BOE núm. 295 de 10.12.2007; MP: Pablo Pérez Tremps), respecto del acceso a los datos almacenados en un teléfono móvil, si bien declarando vulnerado en tal caso el art. 18.3 CE al haberse accedido por la Guardia Civil al registro de llamadas memorizado en el terminal intervenido al recurrente, confeccionando un listado de llamadas recibidas, enviadas y perdidas, sin su consentimiento ni autorización judicial.

utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información[14].

2. ANTECEDENTES

Diversas disposiciones a nivel europeo se han ocupado de esta materia. Así puede citarse en primer lugar el Convenio núm. 108 del Consejo de Europa sobre protección de los datos informatizados de carácter personal[15], y las recomendaciones del Comité de Ministros que lo desarrollan, en particular, la recomendación sobre datos personales utilizados en el sector policial[16] y la recomendación sobre privacidad en Internet[17]. El preámbulo de esta última recomendación dispone que "el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las «autopistas de la información» suponen riesgos para la intimidad de las personas naturales" y que "las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto a la intimidad y del secreto de las comunicaciones, tal y como se garantizan en el art. 8 CEDH[18]". Además, recuerda esta recomendación que "el uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad", por cuanto cada visita a un sitio de Internet deja una serie de "rastros electrónicos" que pueden utilizarse para establecer "un perfil de su persona y sus intereses", subrayando también que la dirección de

[14] Tal conclusión parece desprenderse, si bien de manera indirecta, de la STC 34/2009, Sala 2ª, de 9.02.2009 (BOE núm. 63 de 14.03.2009; MP: Vicente Conde Martín de Hijas), en la que apreciaba que no se había infringido por el órgano judicial el principio de legalidad penal al haber condenado al demandante por un delito de descubrimiento y revelación de secretos, cuyo bien jurídico protegido es la intimidad, resultando como hechos probados que este había accedido al ordenador de una compañera de trabajo y había procedido a la lectura de sus mensajes de correo electrónico. En particular, reseñaba que "desde la estricta perspectiva de control que corresponde a este Tribunal en modo alguno cabe tildar a la vista del tipo penal previsto del art. 197.1 y 2 CP de aplicación analógica o *in malam partem*, carente de razonabilidad por apartarse de su tenor literal o por utilización de pautas extravagantes o criterios no aceptados por la comunidad jurídica la llevada a cabo por la Audiencia Provincial, al considerar documentos personales e íntimos la libreta de direcciones y de teléfonos de la denunciante, accediendo por este medio a la dirección de su correo electrónico y subsumir en aquel tipo penal el acceso a dichos documentos sin el consentimiento de su titular, obteniendo de esta forma datos de carácter personal de aquella y de sus compañeros, que es la conducta por la que ha sido condenado el recurrente de amparo".

[15] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28.01.1981, ratificado por España el 27.01.1984 (BOE núm. 274, de 15.11.1985)

[16] Recomendación Núm. (R) 87, 15, adoptada en Comité de Ministros de 17.09.1987.

[17] Recomendación Núm. (R) 99, 5, adoptada en Comité de Ministros de 23.02.1999.

[18] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4.11.1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6.05.1963 y 20.01.1966, respectivamente (BOE núm. 243, de 10.10.1979).

correo electrónico constituye "un dato de carácter personal que otras personas pueden querer utilizar para diferentes fines".

En este mismo orden de cosas debe citarse la acción normativa desarrollada por la Unión Europea, entre la que destaca, además de la consagración del derecho a la protección de los datos personales realizada por el art. 8 CDFUE[19], la Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[20], cuyo considerando núm. 6 resalta que "Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad". Además, recuerda que "los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el CPDHLF[21]", advirtiendo que "los denominados programas espías (*Spyware*), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intromisión en la intimidad de dichos usuarios".

También cabe citar las resoluciones del Parlamento Europeo de 17.09.1996[22] y 17.12.1998[23], ambas sobre el respeto de los derechos humanos en la Unión Europea, la primera en cuanto dispone en su apartado 53 que "el respeto de la vida privada y familiar, de la reputación, del domicilio y de las comunicaciones privadas, tanto de las personas físicas como jurídicas, así como la protección de datos de carácter personal son derechos fundamentales básicos respecto de los cuales los Estados miembros deben ejercer una especial protección, habida cuenta de la incidencia negativa que sobre los mismos tienen las nuevas tecnologías y que sólo la armonización de las legislaciones nacionales en la materia, confiriendo una alta protección, es susceptible de responder a este desafío"; y la segunda, al subrayar en su apartado 23 que "el

[19] Carta de los Derechos Fundamentales de la Unión Europea (DOUE núm. 83, de 30.03.2010).

[20] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12.07.2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas –Directiva sobre la privacidad y las comunicaciones electrónicas- (DOUE núm. 201, de 31.07.2002).

[21] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4.11.1950, y enmendado por los Protocolos adicionales núm. 3 y 5, de 6.05.1963 y 20.01.1966, respectivamente (BOE núm. 243, de 10.10.1979).

[22] Resolución de 17.09.1996, sobre los derechos humanos en la Unión (DO C 320 de 28.10.1996)

[23] Resolución, de 17.12.1998, sobre el respeto de los derechos humanos en la Unión Europea (DO C 98 de 9.4.1999).

derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia, así como a la protección de los datos de carácter personal, representan derechos fundamentales que los Estados tienen la obligación de proteger y que, por consiguiente, toda medida de vigilancia óptica, acústica o informática deberá adoptarse dentro de su más estricto respeto y acompañada en todos los casos de garantías judiciales".

El TJUE[24] ha reafirmado también la importancia del derecho a la protección de los datos personales como un elemento a tomar en consideración no sólo en el momento de transponer una directiva sino también cuando las autoridades estatales y los órganos judiciales nacionales procedan a su aplicación. Por su parte, el TEDH[25] ha venido asumiendo una interpretación extensiva del concepto "vida privada" del art. 8 del CPDHLF. Así, considera que el término "vida privada" no se debe interpretar de forma restrictiva, de forma que este "engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes", sin que "ninguna razón de principio permita excluir las actividades profesionales o comerciales"[26]. De manera específica, considera que están incluidos en el ámbito de protección del art. 8 CPDHLF, por cuanto pueden contener datos sensibles que afecten a la intimidad, tanto los correos electrónicos enviados desde el lugar del trabajo como la información derivada del seguimiento del uso personal de Internet[27]. Asimismo consideró que el registro de la oficina de un Abogado, incluyendo los datos electrónicos, equivale a una injerencia en su vida privada, lesiva por ello del art. 8 del Convenio[28]. De lo expuesto, parece desprenderse que cualquier injerencia en el contenido de un ordenador personal, ya sea por vía de acceso remoto a través de medios técnicos, ya por vía manual, deberá venir legitimada en principio por el consentimiento de su titular, o bien por la

[24] Entre otras, STJUE, Gran Sala, de 29.01.2008 (Asunto C-275/06, Productores de Música de España c. Telefónica de España SAU; MP: J. Malenovský).

[25] STEDH de 16.02.2000 (Núm. 27798/95, Amann c. Suiza).

[26] T. FREIXES SAN JUAN, "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos", en Y. GÓMEZ SÁNCHEZ (coord.) / A. TORRES DEL MORAL, et al., *Los Derechos en Europa*, UNED, Madrid, 2001, pp. 446-453.

[27] STEDH de 3.04.2007 (Núm. 62617/00, Copland c. Reino Unido). En este caso, precisa el Tribunal, a la demandante no se le advirtió de que podría ser objeto de un seguimiento, por lo que podía razonablemente esperar que se reconociera el carácter privado "en lo que respecta al correo electrónico y la navegación por Internet".

[28] STEDH de 22.05.2008 (Núm. 65755/01, Iliya Stefanov c. Bulgaria). No obstante reconoce el Tribunal que concurría en este caso un objetivo legítimo –investigación penal por delito de extorsión–, y que existía una previa autorización judicial, siendo así que "los registros del PC y las incautaciones deben, por regla general, llevarse a cabo en virtud de una orden judicial", razona que la expresada orden se había elaborado en términos excesivamente amplios, ejecutándose además de manera desproporcionada por la policía, por lo que se había afectado al secreto profesional, por cuanto "retiró todo el equipo del solicitante, incluyendo sus accesorios, así como todos los disquetes que se encontraban en su oficina", resultando que durante el tiempo que permaneció este material en su poder "ningún tipo de garantías existen para asegurar que durante el periodo intermedio el contenido completo del disco duro y los discos no fueron inspeccionados o copiados".

concurrencia de los presupuestos habilitantes antes citados[29].

Esta normativa ha sido recogida en el nuevo capítulo VIII del Título octavo de la LECRIM, tras la reforma efectuada por la LO 13/2015[30], que establece una regulación específica de la materia objeto de estudio, presidida por el principio de la necesidad de autorización judicial, y que analizaremos en los siguientes epígrafes. Como se establece en la exposición de motivos, la reforma "descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido".

3. AUTORIZACIÓN JUDICIAL

Esta autorización será precisa tanto en los supuestos en los que los dispositivos se ocupen durante un registro domiciliario, como en los incautados fuera del domicilio del investigado, sin perjuicio de que la misma pueda ser otorgada con posterioridad al acceso. Así lo establecen los nuevos arts. 588 sexies a y b LECRIM, tras la reforma operada por la referida LO 13/2015. 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[31]. La consideración de cada uno de estos datos de forma separada y con un régimen de protección diferenciado es insuficiente para garantizar una protección eficaz, pues resulta muy difícil asegurar que una vez permitido el acceso directo de los agentes policiales a estos instrumentos para investigar datos únicamente protegidos por el derecho a la intimidad –por ejemplo, los contactos incluidos en la agenda–, no se pueda acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. Es por ello por lo que el Legislador otorga un tratamiento unitario a los datos contenidos en los

[29] Más ampliamente, P. SANTOLAYA MACHETTI, "Limitación a la aplicación de las restricciones de derechos: un genérico límite a los límites según su finalidad", en J. GARCÍA ROCA / P. SANTOLAYA MACHETTI (Coords.), et al., *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2005, p. 758; y R. CASANOVA MARTÍN, "Valoración crítica de las intervenciones telefónicas en el borrador de Código Procesal Penal", en V. MORENO CATENA (Dir.) / C. RUIZ LÓPEZ, (Coord.), et. al., *Reflexiones sobre el nuevo proceso penal: Jornadas sobre el borrador del nuevo Código Procesal Penal*, Tirant lo Blanch, Valencia, 2015, p. 544. P. SANTOLAYA MACHETTI, "Limitación a la aplicación de las restricciones de derechos: un genérico límite a los límites según su finalidad", en J. GARCÍA ROCA / P. SANTOLAYA MACHETTI (Coords.), et al., *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2005, p. 758.

[30] LO 13/2015, de 5 de octubre, de modificación de la LECRIM para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE núm. 239, de 6.10.2015).

[31] Por ejemplo, ccomunicaciones a través de sistemas de mensajería, tuteladas por el art 18 3º CE; contactos o fotografías, 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.

ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual.

El TS[32] ha declarado que el acceso de los poderes públicos al contenido del ordenador de un investigado, 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 datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos. Pero su contenido también puede albergar 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. Conforme establece el TEDH[33] 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 policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al investigado 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.

La ponderación judicial de las razones que justifican, en el marco de

[32] SSTS, Sala 2ª, de 18.07.2014 (ROJ: STS 3086/2014; MP: Manuel Marchena Gómez); 17.04.2013 (ROJ: STS 2222/2013; MP: Manuel Marchena Gómez); y 13.10.2009 (ROJ: STS 6139/2009; MP: José Manuel Maza Martín).

[33] La STEDH de 3.04.2007 (núm. 62617/00, Copland c. Reino Unido), advierte que el acceso a correos electrónicos ya leídos almacenados en la memoria de un PC no afectaría al derecho al secreto de las comunicaciones, sino a la intimidad "en la medida que estos correos o email, escritos o ya leídos por su destinatario, quedan en la memoria del terminal informático utilizado".

una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris propi*o, 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.

Así lo ha recogido expresamente el legislador en la LO 13/2015 de 5 de octubre que ha introducido en el título III del Libro II de la LECRIM un Capítulo VII "registro de dispositivos de almacenamiento masivo de información". Comienza este capítulo haciendo referencia al supuesto de un registro domiciliario en el que sea previsible se incauten ordenadores instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo, en cuyo caso la autorización judicial deberá extenderse a estos extremos justificando las razones que legitimen el acceso a los mismos y su información. Por tanto la incautación no es suficiente para poder acceder a su contenido aunque este acceso se pueda autorizar ulteriormente por el juez competente.

Sentada la necesidad de mandamiento judicial para el acceso a los contenidos en los equipos informáticos en cualquier instrumento de almacenamiento de información, cabe preguntarse si la resolución en la que se acuerde la entrada y registro del domicilio debe de ser tan específica que contenga dicha concreción o bien es suficiente que cuando la petición de acceso a los ordenadores y demás dispositivos de

información digital ha sido solicitada en el oficio de la policía, la concesión del auto de entrada y registro sin establecer ningún tipo de limitación ha de entenderse suficiente. La entidad de los derechos que se están limitando hace que sea no sólo conveniente sino necesario el que la resolución que autorice la entrada y registro del domicilio habilite de manera expresa para la inspección de los ordenadores. Se debe partir de la base que el auto de entrada y registro en el domicilio es un auto que autoriza para entrar en un espacio físico, pero que los ordenadores y todos aquellos aparatos susceptibles de contener una información íntima y personal, relativa a la vida privada de una persona, que contienen o pueden contener datos referidos a la salud, aficiones personales, tendencias sexuales, ideologías, creencias religiosas, inciden de manera directa en la esfera más íntima de los ciudadanos, y sobre la cual existe un derecho de exclusión, que sólo se vence con una resolución judicial en los supuestos contemplados en la ley. Por ello se hace preciso, en la medida en que lo que se trata de examinar es ese espacio virtual privado, distinto y con entidad propia al domicilio, una resolución habilitante para el acceso a estos aparatos. De lo que se trata es, una vez reconocida la inviolabilidad del entorno digital como una manifestación del derecho a la intimidad, que ese reconocimiento tenga una trascendencia jurídica, que en este caso sería la habilitación específica. De lo contrario, todo lo más que se podría hacer sería la incautación del material que contenga la información para, una vez obtenida la resolución habilitante, proceder a su estudio y análisis.

Distinto a este supuesto es el de la autorización para la incautación de efectos. En este caso, lo que se plantea es si la autorización para la entrada y registro del domicilio habilita para la intervención de los efectos que en la misma se encuentren, o si por el contrario se precisa que el auto de entrada y registro habilite para ello de manera expresa. Entendemos que por la naturaleza y finalidad del registro, como diligencia sumarial, es la de averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación, así como la identidad de los delincuentes. Tiene una naturaleza instrumental en la medida en que tiene por objeto el acopio de los elementos de prueba que sirvan para acreditar la existencia del delito y la imputación a sus responsables. De ahí que se redacte un acta en la que se hace constar el resultado de la diligencia así como los objetos que se hayan intervenido. De lo que se deduce que es consustancial al auto en el que se autoriza la entrada y registro en un domicilio la habilitación para intervenir cualquier tipo de efectos o instrumentos, entre los que se encuentran los dispositivos de almacenamiento de información digital. Esta cuestión se planteó y fue resuelta por el TS[34] entendiendo que la necesidad de que toda resolución judicial llamada a legitimar un acto de injerencia en los derechos fundamentales del investigado sea interpretada conforme a su estricta literalidad, forma parte de las notas definitorias de nuestro sistema

[34] STS, Sala 2ª, de 17.04.2013, cit., conforme a la cual, "nada de ello se desprende de la literalidad de aquel precepto –art. 476 LECRIM–".

constitucional. En esta materia no caben las interpretaciones extensivas ni la elasticidad como fuente inspiradora a la hora de delimitar los exactos términos de la autorización concedida. Nuestro sistema no ampara autorizaciones implícitas, ni mandamientos de intromisión en el espacio de exclusión que definen los derechos fundamentales que no estén dibujados con la suficiencia e indispensable claridad. Sin embargo, este irrenunciable punto de partida no está reñido con la necesidad de relacionar el documento policial en el que se postula la concesión de la autorización y el acto jurisdiccional habilitante. Sólo así podrá concluirse si lo que se concede es lo mismo que lo que se pide o si, por el contrario, la decisión jurisdiccional restringe o pone límites a la petición cursada. Ahora bien, carecería de todo sentido, que si en la fundamentación jurídica del auto de entrada y registro nada se menciona al respecto que la autorización judicial se limitara a facultar a los agentes a la práctica de una inspección ocular que les permitiera averiguar la existencia de los equipos técnicos desde los que se estaba cometiendo un delito y que, una vez averiguada esa existencia, se obligara a los agentes a marcharse del domicilio registrado, dejando esos elementos de prueba de primer orden en poder del investigado. No cabe duda alguna de que esa averiguación sólo adquiere sentido como medio para, una vez constatada su existencia, intervenir lo que no serían sino instrumentos de unos delitos para cuyo esclarecimiento se había concedido, precisamente, el mandamiento de entrada y registro. En definitiva, desde este punto de vista, es claro que para averiguar si los ordenadores y demás dispositivos intervenidos tenían o no relación con el delito que estaba siendo objeto de investigación, resultaba indispensable su intervención y, claro es, su ulterior examen.

En consecuencia la regulación vigente de la LECRIM distingue, de una parte, la aprehensión y ocupación de efectos llevadas a cabo durante el registro domiciliario, para lo que es suficiente la resolución judicial que legitima la entrada y registro en el domicilio, de lo que es el acceso a dispositivos de almacenamiento masivo de información, para lo cual se precisa que el Juez lo autorice de manera expresa, bien en la misma resolución en la que acuerde el registro, justificando dicho acceso, bien en otra posterior independiente. Queda así regulado el acceso a los dispositivos electrónicos sobre lo que había una jurisprudencia no suficientemente clara[35] que salvaba sin embargo siempre los supuestos de

[35] Así la STS, Sala 2ª, de 7.11.2013 (ROJ: STS 5515/2013; MP: Joaquín Giménez García), con referencia a la Circular FGE 1/2013, entendió que la apertura de archivos de un disco duro o de unidades externas tampoco afecta al derecho al secreto de las comunicaciones. Se considera más bien el cuerpo de los delitos informáticos. En base a ello considera que no es en todo caso imprescindible la autorización judicial, a salvo, el acceso a correos electrónicos. Los documentos no integrados en un proceso de comunicación y almacenados en archivos informáticos bien en teléfonos móviles, ordenadores o asimilados, tendrían la consideración de simples documentos y, por tanto, sólo resultarían, en su caso protegidos por el derecho a la intimidad. Por ello entiende que los Cuerpos y Fuerzas de Seguridad del Estado pueden, sin autorización judicial, intervenir un soporte magnético o electrónico, como, por ejemplo, la lectura de un disco duro, aun cuando su contenido material pudiera afectar al derecho a la intimidad del art. 18.1 CE, si se aprecian razones de urgencia y se persigue un interés constitucionalmente

urgencia, especialmente en materias que afecten a menores[36].

La resolución judicial que acuerde la autorización de esta medida de investigación deberá tomar en consideración los principios rectores establecidos en el nuevo art 588 bis a) LECRIM, atendiendo a que, como señala expresamente la exposición de motivos de la LO 13/2015, constituyen la proclamación normativa de unos principios que el TC[37] ya había definido como determinantes de la validez de los actos de injerencia en la privacidad del investigado en un proceso penal.

Especialidad. Este principio exige que una medida esté relacionada con la investigación de un delito concreto, sin que puedan autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva. La necesaria represión de conductas delictivas graves, el ejercicio del *ius puniendi* del Estado y la nueva criminalidad organizada, no pueden permitir en absoluto la que se ha denominado como investigación prospectiva o *causa generalis*[38]. Por tanto, la medida deberá tener por finalidad investigar un hecho que integre el objeto del proceso penal, y no meros indicios o sospechas. En palabras del TC "un acto instructorio que limite un derecho fundamental no puede estar dirigido exclusivamente a obtener meros indicios o sospechas de criminalidad, sino debe tener como finalidad la preconstitución de la prueba de los hechos que integran el objeto del proceso penal"[39].

Idoneidad. Debe existir una relación de adecuación entre el acceso al dispositivo electrónico y el fin que se pretende. De esta forma, aquél debe servir objetivamente para la finalidad constitucionalmente legítima, esto es, conseguir datos útiles para investigar las circunstancias del delito. La cuestión de la idoneidad, consiguientemente, no depende de la concreción del peligro, sino exclusivamente de la abstracta adecuación al mismo que ha establecido el legislador[40]. Este principio sirve para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.

Excepcionalidad. De la nota de excepcionalidad se deriva que el

---

legítimo con base en la habilitación legal para dicha actuación reconocida en los arts. 282 LECRIM y 11.1 LO 2/1986 de 13 de Marzo, de Fuerzas y Cuerpos de Seguridad, y 547 LOPJ". En similar sentido SSTS, Sala 2ª, de 26.12.2013 (ROJ: STS 6486/2013; MP: Luciano Varela Castro); y 3.10.2007 (ROJ: STS 6379/2007; MP: Miguel Colmenero Menéndez de Luarca).

[36] SSTS, Sala 2ª, de 21.03.2011 (ROJ: STS 1864/2011; MP: Joaquín Jiménez García); y 29.07.2011 (ROJ: STS 6062/2011; MP: Joaquín Giménez García).

[37] SSTC 222/2012, Pleno, de 27.11.2012 (BOE núm. 313 de 29.12.2012; MP: Luis Ignacio Ortega Álvarez); y 12/2008, Pleno, de 29.01.2008 (BOE núm. 52 de 29.02.2008; MP: Elisa Pérez Vera).

[38] J. L. GONZÁLEZ-MONTES SÁNCHEZ, "Reflexiones sobre el Proyecto de Ley Orgánica de Modificación de la LECRIM para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", en *Revista electrónica de ciencia penal y criminología*, núm. 17, 2015, p. 27.

[39] STC 207/1996, Sala 1ª, de 16.12.1996, cit. En similar sentido, SSTC 165/2005, Sala 2ª, de 20.06.2005 (BOE núm. 173 de 21.07.2005; MP: Vicente Conde Martín de Hijas); y 26/2006, Sala 2ª, de 30.01.2006 (BOE núm. 51 de 1.03.2006; MP: Guillermo Jiménez Sánchez).

[40] STS, Sala 2ª, de 7.09.2015 (ROJ: STS 3981/2015; MP: Antonio del Moral García).

registro de estos dispositivos no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado. Ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria. Ciertamente en la mayoría de los supuestos de petición se estará en los umbrales de la investigación judicial, normalmente tal petición irá conjuntamente con la solicitud de una entrada y registro, pero en todo caso debe acreditarse una previa y suficiente investigación policial que para avanzar necesita, por las dificultades del caso, de la intervención de los dispositivos. Por ello la nota de la excepcionalidad, se completa con las de idoneidad y necesidad y subsidiariedad formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional[41].

Necesidad. El acceso ha de resultar imprescindible para cumplir el éxito de la investigación pretendida y no se ofrezcan otros instrumentos que, siendo igualmente operativos, resulten menos injerentes en el núcleo esencial del derecho individual que se limita. En definitiva, nos encontramos ante una cláusula de subsidiariedad, de tal manera que el medio seleccionado para alcanzar el fin no pueda ser suplido por otro igualmente eficaz, pero que no restrinja el derecho fundamental o lo haga de una manera menos gravosa[42]. La ponderación mesurada entre, de un lado, el interés particular del sospechoso a que se respete su vida privada y familiar y, de otro, el interés general contrapuesto del Estado en defender el orden, bien para investigar y castigar delitos cometidos, bien para prevenir la comisión de otros en el futuro, bien para salvaguardar los derechos de terceros que, como los menores, pueden ser especialmente vulnerables. En relación con lo cual, lógicamente, el carácter delictivo de la conducta de la persona afectada por la restricción no es en absoluto irrelevante en la balanza, pues el contexto y el comportamiento de la víctima –de la injerencia en su intimidad–, juegan un rol determinante en la apreciación de la licitud de la injerencia. La necesidad en una sociedad democrática significa que la necesidad ha de ser imperiosa y la respuesta proporcionada a la finalidad perseguida. Nadie puede dudar de que la pornografía infantil concita un severísimo reproche social. Ni tampoco nadie puede cuestionarse la alarma que genera el uso perverso de Internet para consumirla, producirla y distribuirla sirviéndose del anonimato. El reclamo social o la alarma ciudadana no bastan por sí mismos, en cambio, para justificar cualquier medida[43]. La necesidad es,

[41] STS, Sala 2ª, de 31.05.2016 (ROJ: STS 2586/2016; MP: Francisco Monteverde Ferrer).

[42] E. PEDRAZ PENALVA / V. ORTEGA BENITO, "El principio de proporcionalidad y su configuración en la jurisprudencia del TC y literatura especializada alemanas", en *Poder Judicial*, núm. 17, 1990, p. 17.

[43] En este orden de ideas, el TEDH ha establecido que la buena fe no es suficiente para justificar medidas de este calado y que no basta, desde luego, con que sean ventajosas –STEDH de 7.12.1976 (Series A núm. 24, *Handyside c.* Reino Unido)–, ni tampoco, por supuesto, es de recibo considerar necesarias medidas de esta índole sólo porque sean

sin duda, un test de control más severo cuyo rigor se modula en función de la propia naturaleza del derecho afectado, de las actividades en juego y de la finalidad de la restricción.

Proporcionalidad. Este principio tiene como finalidad la determinación, mediante la utilización de las técnicas del contrapeso de los bienes o valores y la ponderación de intereses según las circunstancias del caso concreto, si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés estatal que se trata de salvaguardar[44]. Para que el acceso al dispositivo electrónico resulte proporcional en el caso concreto, deben tenerse en cuenta varios criterios[45]. En primer lugar, el criterio de la expectativa de las consecuencias jurídicas del delito, es decir, deberá tenerse en cuenta la gravedad de la pena señalada al delito que se está investigando[46]. En segundo lugar, el criterio de la importancia de la causa que, entre otras circunstancias, viene determinada por la naturaleza del bien jurídico lesionado, las concretas formas de manifestación del hecho –la habitualidad en la comisión delictiva, la peligrosidad social de los efectos del hecho, etc. –, y las circunstancias relevantes en la persona del investigado, esto es, la tendencia a cometer hechos de la misma naturaleza o la especial intensidad del comportamiento delictivo[47]. Finalmente, el criterio del grado de imputación. El Estado podrá restringir un derecho fundamental sólo en aquellos supuestos en los que exista un grado suficiente de imputación de un delito, es decir, cuando existan razones objetivas que permitan afirmar la probabilidad de que se haya cometido un delito. En otro caso, se estaría otorgando a los órganos estatales una patente de corso para inmiscuirse en la vida privada de los ciudadanos inadmisible en un Estado de Derecho.

4. TÉRMINOS, ALCANCE, CONDICIONES Y GARANTÍAS DEL REGISTRO.

Conforme a lo ya expuesto, el nuevo régimen legal hace que el acceso al contenido de ordenadores, instrumentos de comunicación telemática o dispositivos de almacenamiento masivo de información digital, o a repositorios telemáticos de datos, que se pudieran aprehender con ocasión de un registro domiciliario, o fuera de él, precise de previa autorización judicial. Esta autorización judicial ha de fijar los términos y alcance del

útiles u oportunas –STEDH de 13.08.1971 (Series A núm. 44, *Young, James y Webster* c. Reino Unido)–.

[44] N. GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid, 1990, p. 225.

[45] La STC 66/1995, Sala 2ª, de 8.05.1995 (BOE núm. 140 de 13.06.1995; MP: Carles Viver Pi-Sunyer), importó, por primera vez, el calificado como triple test de proporcionalidad, de origen alemán, dando a conocer la fórmula que en adelante empleará el TC para resolver las limitaciones de derechos que se elevaran a su conocimiento.

[46] M. GONZÁLEZ BEILFUSS, El *principio de proporcionalidad en la jurisprudencia del TC*, Aranzadi, Navarra, 2015, pp. 309-310.

[47] J. F. ETXEBERRÍA GURIDI, "La inadmisibilidad de los tests masivos de ADN en la investigación de los hechos punibles", en *Actualidad Penal*, núm. 28, 1999, nota 39.

registro, la posibilidad de hacer copias de los datos informáticos, así como las condiciones a que se habrá de sujetar para asegurar la integridad de los datos y las garantías de preservación que sean precisas para hacer posible, en su caso, un ulterior análisis pericial.

Por tanto, el acceso a los dispositivos de almacenamiento masivo podrá ser limitado a determinados dispositivos o carpetas. La información almacenada en un dispositivo se puede discriminar en atención a su titularidad y a la clase de dato. Como regla general, el registro afectará a datos relativos al sujeto investigado, siendo irrelevante donde se encuentren alojados, esto es, si el dispositivo le pertenece, como será lo habitual, o es de un tercero, salvo que existan razones que justifiquen que el registro recaiga sobre la totalidad de los datos almacenados con independencia de su titularidad. Por otro lado y habida cuenta de las distintas clases de datos que pueden encontrarse almacenados en un dispositivo esa especificación puede extenderse también a este aspecto, concretándose el tipo de información a que se puede acceder[48].

Mediante la fijación obligatoria de las condiciones que aseguren la integridad de los datos volcados se pretende asegurar que no existe alteración ni manipulación de las fuentes de prueba[49]. Estas garantías legales no son más que emanaciones concretas del derecho a un proceso con las garantías debidas así como del propio derecho fundamental a la defensa, y es que, la verdadera cuestión a dilucidar aquí es la del valor atribuible, desde la perspectiva de su autenticidad, a la prueba electrónica[50].

La resolución judicial habrá de concretar, entre otros extremos, si se autoriza la realización de un clonado o volcado, que consiste en la realización de una "copia espejo" o bit a bit de la información original, o bien la realización de una copia lógica, es decir, una copia selectiva de ciertas carpetas o ficheros. Todo el proceso de volcado[51] comienza etiquetando e inventariando todos los dispositivos que se van a analizar: discos duros, pendrives, cámaras, etc. De forma genérica se puede

[48] N. CABEZUDO RODRÍGUEZ, "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", en *Boletín del Ministerio de Justicia*, núm. 2186, 2016, pp. 39-47.

[49] La conservación de la cadena de custodia es vital para las garantías procesales del investigado, ya que si en un examen forense posterior a la intervención domiciliaria, se detecta que las pruebas o dispositivos informáticos están o pueden estar contaminados, se podría llegar a cuestionar o, incluso, invalidar todo el proceso. En este sentido, STS, Sala 2ª, de 3.12.2012 (ROJ: STS 8316/2012; MP: Luciano Varela Castro).

[50] Voto particular del Magistrado Manuel Marchena Gómez, al que se adhiere José Manuel Maza Martín, en STS, Sala 2ª, de 30.12.2009 (ROJ: 8417/2009; MP: José Antonio Martín Pallín). C. SANCHÍS CRESPO, "La prueba en soporte electrónico", en E. GAMERO CASADO / J. VALERO TORRIJOS, et al., *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*. Aranzadi, Navarra, 2012, p. 713, define prueba electrónica o en soporte electrónico 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".

[51] A. MARTÍNEZ RETENAGA, *Guía de toma de evidencias en entornos Windows*, Instituto Nacional de Ciberseguidad, Ministerio de Industria, Energía y Turismo, 2014, pp. 1-80.

clasificar el tipo de información a recopilar en dos grandes grupos: información volátil[52] e información no volátil. Asimismo, se puede hablar de *live acquisition*, que corresponde a la obtención de información en un sistema en funcionamiento, o *static acquisition*, que corresponde a la obtención de información de un sistema que está apagado. Para realizar una correcta obtención de evidencias es importante el uso de software no invasivo y que se encuentre en dispositivos protegidos contra escritura[53]. Técnicamente la autenticidad de la copia objeto de volcado se consigue contrastando el resumen digital recogido sobre la prueba original, basado en algoritmos *hash[54],* con el de la copia sobre la que se va a emitir la pericia. Es esta prueba técnica de contraste[55] la que garantiza la correcta realización o no del volcado. Si coinciden, el material original y del volcado son idénticos[56].

4.1. Presencia del letrado de la administración de justicia

La nueva regulación guarda silencio sobre la necesidad o no de que las operaciones de volcado se lleven a cabo ante fedatario público[57]. Aunque la misma se ha venido dando por la práctica de los tribunales, existen

[52] La información volátil puede resultar muy importante a la hora de realizar un análisis forense ya que puede contener evidencias de conexiones, de procesos en ejecución, etc. Lo primero que se debe obtener es la fecha y hora del sistema para poder establecer una línea temporal de recopilación de evidencias, duración del proceso, etc. Se debe comparar la fecha obtenida con el tiempo universal coordinado –UTC–, estándar de tiempo por el cual se regula la hora nivel mundial, para determinar si la fecha establecida en el sistema es correcta o no, y que desviación existe.

[53] La conservación de la cadena de custodia en un disco duro o memoria de almacenamiento masivo es una cuestión delicada. Baste señalar que la mera conexión de un disco duro o memoria USB a un ordenador personal para proceder a su análisis, sin necesidad de interactuar con el disco, contamina la prueba de forma irremediable. Para evitar esta contaminación, es necesario el uso de bloqueadoras de escritura, que son dispositivos que actúan como puente entre el disco duro o memoria y el ordenador, de tal forma que el disco o memoria nunca se conectan directamente al ordenador, sino a la bloqueadora, siendo esta la que se conecta finalmente a la máquina.

[54] Un hash es un valor que identifica datos de forma unívoca. Existen distintos tipos de hashes: MD5, SHA-1, SHA-2, etc. El uso del hash MD5, pese al alto grado de utilización, presenta el problema de que pueden surgir colisiones, es decir, puede darse el caso de que ficheros diferentes tengan el mismo MD5, por lo que puede quedar en entredicho la validez de las pruebas. Es por ello que es recomendable que vaya cayendo en desuso. Un caso similar, aunque no igual, es el del SHA-1 por lo que se aconseja que se busquen otras alternativas como SHA-256, SHA-512, etc.

[55] Cualquier modificación del contenido del soporte durante el análisis, por mínima que fuera, arrojaría un *hash* diferente del original. De lo que se deduce que si ambos resúmenes (anterior y posterior al análisis pericial) coinciden, queda demostrada técnicamente la integridad del soporte durante el análisis.

[56] En relación con la incorporación de los documentos electrónicos al proceso, A. E. GUDÍN RODRÍGUEZ-MAGARIÑOS, "Incorporación al proceso del material informático intervenido Durante la investigación penal", en *Boletín del Ministerio de Justicia*, núm. 2163, febrero 2014, pp. 8-13.

[57] M. MARCHENA GÓMEZ / N. GONZÁLEZ-CUÉLLAR SERRANO, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015, p. 375 sugieren que aunque no se prevea en la norma el instructor podrá ordenar que ese volcado de datos se lleve a cabo en presencia del Letrado de la Administración de Justicia.

numerosas SSTS[58] que no la consideran necesaria porque "ninguna garantía podría añadirse con la presencia del Secretario Judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia"[59]. Recientemente el TS[60] se ha vuelto a pronunciar sobre este particular, exponiendo que la jurisprudencia establece que la presencia de este fedatario en el acto del volcado de datos no actúa como presupuesto de validez, por cuanto lo decisivo es despejar cualquier duda sobre la integridad de los datos que contenía, garantizar la correlación entre la información aprehendida en el acto de intervención del dispositivo y la que se obtiene en la diligencia de acceso al aparato. La incorporación de los soportes informáticos debe hacerse en condiciones que preserven su identidad plena y la integridad del contenido de lo intervenido[61], pues "aunque no hay duda de que el Secretario Judicial es una instancia formal de garantía, la jurisprudencia aconseja no sobrevalorar su mediación, por su propia condición de profano en materia de conocimientos informáticos".

No obstante lo anterior, aún en el caso de no compartirse la innecesaridad de tal presencia[62], hemos de insistir que la misma en ningún caso es requisito de validez de la prueba, de tal manera que su

[58] SSTS, Sala 2ª, de 22.05.2009 (ROJ: STS 3057/2009; MP: Juan Ramón Berdugo Gómez de la Torre), caso Ekin-Kas-Xaki; y 14.05.2008 (ROJ: STS 2809/2008; MP: Perfecto Agustín Andrés Ibáñez), conforme a la cual "es cierto que esta última actividad -se refiere al análisis de la información de ordenadores incautados en su registro domiciliario autorizado judicialmente- no fue practicada ante el Secretario Judicial, sino por los técnicos policiales en su propia sede. Pero también lo es que, esa presencia que se reclama habría sido, de facto, tan inútil -y, por tanto, innecesaria- como la que pudiera darse en el desarrollo de cualquier otra de las muchas imaginables en cuya técnica el fedatario judicial no fuera experto".

[59] STS, Sala 2ª, de 15.11.1999 (ROJ: STS 7208/1999; MP: José Antonio Martín Pallín), que asimismo manifiesta que "lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia". En este sentido, J. A. BONILLA CORREA , "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio (1)", en *Diario La Ley*, núm. 8522, 20.04.2015, p. 12, considera que "sólo en aquellos casos de intervenciones extremadamente excepcionales, si el Secretario Judicial entiende que su presencia es oportuna, estará presente en el inicio de la diligencia de clonado, por analogía a los dispuesto en el punto sexto de la Instrucción 6/2013 de la Secretaría General de la Administración de Justicia, relativa a La aplicación del Protocolo sobre Aprehensión, análisis, custodia y destrucción de drogas tóxicas, estupefacientes y sustancias psicotrópicas".

[60] STS, Sala 2ª, de 14.04.2015 (ROJ: STS 1922/2015; MP: Francisco Monteverde Ferrer).

[61] STC 170/2003, Sala 1ª, de 29.09.2003 (BOE núm. 254 de 23.10.2003; MP: Eugeni Gay Montalvo)

[62] E. VELASCO NÚÑEZ, "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", en *Diario La Ley*, núm. 8183, 4.11.2013, pp. 1001-1012, justifica la necesidad de la presencia del Letrado de la Administración de Justicia, "como garante de la legalidad, en su misión de velar por la fe pública y la custodia original del efecto tecnológico, que debe después guardar precintado".

ausencia no determinaría nunca su nulidad[63]. El volcado practicado sin su presencia dejaría de considerarse, en su caso, como una prueba preconstituida, pero podría llevarse al juicio oral por otras vías, especialmente mediante la declaración de los agentes que realizaron el volcado que será valorada por el tribunal de enjuiciamiento. Conforme ha quedado expuesto anteriormente, existen medios tecnológicos que permiten que garantizar la autenticidad e integridad de la fuente de prueba, como el hash, algoritmo que permite afirmar que los datos que se encontraban en el dispositivo en el momento de su ocupación no han sido objeto de manipulación posterior. Los agentes que realicen el volcado usarán elementos técnicos para garantizar la autenticidad e integridad de los datos, que habrán de documentarse para su incorporación al proceso, por lo que lo relevante es la homologación de equipos y programas, tal y como acontece con las pruebas de alcoholemia. En definitiva, y en cualquier caso, el volcado de los datos es una cuestión de legalidad ordinaria, al no afectar a derechos fundamentales.

Sobre esta cuestión cabe destacar el Acuerdo al que llegó la Comisión Nacional de Coordinación de la Policía Judicial[64] en su reunión de 16.10.2014[65], cuyo tenor literal reproducimos: "Volcados informáticos: apertura o volcado del disco duro y memoria de almacenamiento de datos de los equipos informáticos ante la presencia del Secretario Judicial. El Excmo. Sr. Fiscal General del Estado manifestó que aunque hay alguna sentencia de la Audiencia Nacional en la que exige la presencia del Secretario Judicial para realizar las operaciones indicadas, el TS, en varias sentencias, deja claro que no es precisa la presencia del Secretario Judicial para los fines indicados. La Comisión Nacional de Policía Judicial por unanimidad estuvo de acuerdo con la propuesta del Comité Técnico, en el sentido de no ser necesaria la presencia del Secretario Judicial para la apertura, volcado de disco duro y memoria de almacenamiento de datos de los equipos informáticos".

Ahora bien, y no obstante lo anterior, no ha lugar a duda alguna de que el Letrado de la Administración de Justicia estará siempre presente cuando el volcado se lleve a cabo de manera simultánea durante la práctica de un registro domiciliario, habida cuenta de su necesaria presencia en esta última diligencia –a efectos de que la misma tenga el carácter de prueba preconstituida, no como requisito de validez de la

[63] J. DELGADO MARTÍN, "La prueba electrónica en el proceso penal", en *Diario La Ley*, núm. 8167, 10.10.2013, p. 10.

[64] La Comisión Nacional de Coordinación de la Policía Judicial se creó en 1987 con el fin de armonizar y lograr la unidad de la dirección en las fuerzas adscritas a la investigación criminal. Entre sus atribuciones están la de efectuar estudios acerca de la evolución y desarrollo de la delincuencia, emitir informes o realizar propuestas de planes generales de actuaciones de la Policía Judicial contra la criminalidad y unificar criterios o resolver eventuales incidencias que dificulten el adecuado funcionamiento de esta.

[65] Bajo la presidencia del Presidente del CGPJ y del TS, y asistiendo otros miembros de la Comisión como el Ministro de Justicia, el Ministro del Interior, el Fiscal General del Estado, y un vocal del CGPJ.

diligencia[66]–, así como en el supuesto de que no se proceda a un volcado de datos sino a una copia selectiva de archivos.

4.2. Presencia del interesado y su abogado

Es incuestionable la presencia del interesado en la práctica del volcado cuando sea practicado en unidad de acto con la diligencia de entrada y registro, por cuanto su intervención en el registro es una exigencia prevista en la Ley Procesal –art. 569 LECRIM–, que solo puede excluirse cuando no resulte posible hacer efectiva su asistencia[67], así como cuando se proceda a una copia selectiva de archivos, al no limitarse la diligencia a efectuar un mero proceso técnico de clonación sino a una selección de información susceptible de contradicción. No obstante resulta

[66] Las SSTS, Sala 2ª, de 22.05.2015 (ROJ: STS 2407/2015; MP: Andrés Palomo del Arco); 7.05.2014 (ROJ: STS 1957/2014; MP: Manuel Marchena Gómez); y 18.07.2014 (ROJ: STS 3086/2014; MP: Manuel Marchena Gómez), entre otras muchas, recuerdan que el efecto de la ausencia del Letrado de la Administración de Justicia no se proyecta sobre la validez constitucional de la medida de injerencia. En efecto, el TC –SSTC 239/1999, Sala 1ª, de 20.12.1999 (BOE núm. 17 de 20.01.2000; MP: María Emilia Casas Baamonde); 94/1999, Sala 2ª, de 31.05.1999 (BOE núm. 154 de 29.06.1999; MP: Tomás S. Vives Antón); y 228/1997, Sala 1ª, de 16.12.1997 (BOE núm. 18 de 21.01.1998; MP: Pablo García Manzano)–, viene manteniendo de forma constante que el único requisito necesario y suficiente por sí solo para dotar de licitud constitucional a la entrada y registro de un domicilio, fuera del consentimiento expreso de quien lo ocupa o la flagrancia delictiva, es la existencia de una resolución judicial que con antelación lo mande o autorice, de suerte que, una vez obtenido el mandamiento judicial, la forma en que la entrada y el registro se practiquen, las incidencias que en su curso se puedan producir y los defectos en que se incurra, se inscriben y generan efectos sólo en el plano de la legalidad ordinaria. A este plano corresponde la asistencia del Letrado de la Administración de Justicia cuya ausencia por tanto no afecta al derecho a la inviolabilidad del domicilio ni a la tutela judicial del mismo, aunque sí afecta a la eficacia de la prueba preconstituida por la diligencia. En definitiva, tienen declarado el TC y TS que la ausencia del fedatario público en la diligencia de entrada y registro no afecta al derecho fundamental a la inviolabilidad del domicilio cuando ha precedido la correspondiente resolución que lo autoriza. Cuestión distinta sería la trascendencia que en el orden procesal puede tener la ausencia del Letrado de la Administración de Justicia en tal diligencia. Y es asimismo reiterada la jurisprudencia del TS –SSTS, Sala 2ª, de 18.07.2014 (ROJ: STS 3086/2014; MP: Manuel Marchena Gómez); 27.04.2010 (ROJ: : STS 2135/2010; MP: Francisco Monteverde Ferrer); y 12.04.2006 (ROJ: STS 2057/2006; MP: Juan Ramón Berdugo Gómez de la Torre)–, que proclama que el registro efectuado sin intervención del referido funcionario es procesalmente nulo, careciendo de operatividad y total falta de virtualidad a efectos probatorios, si bien ello no empece a que merced a otros medios de prueba se evidencie la existencia real de los efectos que se dicen intervenidos y hallados en el domicilio registrado.

[67] SSTS, Sala 2ª, de 8.07.2016 (ROJ: STS 3789/2016; MP: José Ramón Soriano Soriano); 7.04.2016 (ROJ: STS 1545/2016; Andrés Martínez Arrieta); y 6.04.2016 (ROJ: STS 1495/2016; MP: Joaquín Giménez García), disponiendo esta última que "ordinariamente el interesado en el registro es el imputado, pues el resultado del registro va a afectar a su defensa , aunque no siempre tiene que estar presente en el registro judicialmente autorizado. El imputado o persona contra la que se dirige el procedimiento puede encontrarse en ignorado paradero, o simplemente fuera de la vivienda y no ser localizable en el momento del registro, ya que la entrada y registro en un domicilio autorizada en el curso de un procedimiento judicial por delito constituye, por su propia naturaleza, una diligencia de carácter urgente que no se puede demorar a la espera de que el imputado regrese a su domicilio o sea localizado policialmente".

controvertido si aquel interesado ha de estar presente cuando se practique el volcado fuera del marco de un registro domiciliario.

La LECRIM, tras la reforma llevada a cabo por la LO 13/2015, contempla como supuestos distintos la detención y apertura de correspondencia y el registro de dispositivos de almacenamiento masivo de información, sometiendo este último a un régimen que no incluye la presencia del investigado ni de su abogado en su apertura[68]. No procede la aplicación analógica de las normas de la LECRIM para la detención y apertura de la correspondencia, que exigen la citación del interesado, a los efectos de que por su abogado se puedan hacer alegaciones e incluso nombrar perito. No siendo tampoco un argumento válido a estos efectos la obsolescencia de la LECRIM con el fin de fundamentar aplicaciones analógicas o extensivas no justificadas de una norma. En los casos de volcados de datos la semejanza –que no la identidad de razón, propia de la analogía-, estribaría en que hay información contenida en un soporte objeto de registro. Sin embargo, el régimen de apertura y examen establecido en los arts. 579 y siguientes LECRIM se funda en que se trata de correspondencia postal o telegráfica, que ha de tener la característica de privada, que físicamente se encuentra dentro de un sobre o similar, y que va a ser examinada por el Juez a fin de tomar conocimiento de lo que interese para la causa, apartando lo demás. En el caso de la información contenida en un dispositivo de almacenamiento masivo, la aprehensión de su contenido es meramente funcional, y no se lleva a cabo una selección, sino que se realiza una copia íntegra a fin de realizar una pericia sobre ese contenido. La presencia del investigado en la diligencia de volcado, en cuanto que no se toma ni aparta nada, sino que consiste meramente en la realización de la copia, no se justifica en dotar de mayor garantía a la operación de volcado[69]. Tampoco puede aducirse que exista el derecho de designar perito para tal diligencia. No entendemos cuál sería la labor de perito a tal efecto. Cuestión distinta es el derecho de la parte a interesar que un perito de su elección analice posteriormente el contenido del dispositivo y realice una pericia. Entender que la presencia del interesado y/o su abogado son necesarios en la práctica del volcado, sería como considerar que los mismos han de estar presente en la práctica de una autopsia, extremo descartado por la jurisprudencia del TS[70].

Si bien no faltan opiniones en sentido contrario[71], entendiendo que,

[68] La STS, Sala 2ª, de 17.04.2013, cit.,

[69] En este sentido, SAP Madrid, Sec. 17ª, de 21.05.2015 (SAP M 6740/2015; MP: Juan José Toscano Tinoco); y SAP A Coruña, Sec. 6ª, de 11.11.2013 (ROJ: SAP C 2875/2013; MP: José Gómez Rey), entre otras.

[70] La STS, Sala 2ª, de 29.01.2013 (ROJ: STS 797/2013; MP: Luciano Varela Castro), acerca de la preceptiva posibilidad de intervención del imputado y su Letrado en la diligencia de autopsia advierte "que la LECRIM no impone la presencia de las partes en la diligencia de práctica material de la autopsia. Al efecto debemos subrayar la diferencia entre lo regulado en los arts. 333 y 336 para las diligencias relativas a inspección ocular y cuerpo del delito, y 340 para el caso de sumarios por causa de muerte violenta, en que se remite al 353 pero no a los anteriores preceptos". En igual sentido STS, Sala 2ª, de 8.09.2003 (ROJ: STS 5423/2003; MP: Miguel Colmenero Menéndez de Luarca).

[71] J. A. BONILLA CORREA, "Los avances tecnológicos…", ob. cit., p. 12.

sobre la base del art. 333 LECRIM, la diligencia de clonado será notificada a las partes en lo referente al lugar y hora en que se realizará. Dicho artículo, bajo la rúbrica de la inspección ocular, dentro del título correspondiente a la comprobación del delito y averiguación del delincuente, establece que cuando "al practicarse las diligencias enumeradas en los artículos anteriores (inspección ocular) hubiese alguna persona declarada procesada, como presunta autora del hecho punible, podrá presenciarlas, ya sola, ya asistida del defensor que eligiese o lo fuese nombrado de oficio, si así lo solicitara", precepto, pues, que no resulta de aplicación a la práctica de la diligencia analizada, que claramente no puede calificarse como de inspección ocular.

4.3. Ausencia de indicaciones en la resolución judicial

Aún cuando conforme a lo ya expuesto resulta exigible que la resolución judicial que autoriza el acceso a la información especifique las condiciones y términos de dicho acceso, no toda irregularidad o infracción de normas procesales es suficiente para provocar una nulidad de actuaciones. Es preciso que de ella se derive un efectivo resultado de indefensión para el investigado. Así lo ha venido declarando el TC[72], entendiendo que para que pueda estimarse una indefensión con relevancia constitucional, que sitúe al interesado al margen de toda posibilidad de alegar y defender en el proceso sus derechos, no basta con una vulneración meramente formal, sino que es necesario que de esa infracción formal se derive un efecto material de indefensión, con real menoscabo del derecho de defensa y con el consiguiente perjuicio real y efectivo para los intereses del afectado. No basta, además, la alegación genérica y abstracta de indefensión, sin concretar cuáles fueron los perjuicios efectivos. El TC[73] ha desestimado reiteradamente la identificación entre defecto o irregularidad procesal e indefensión, pues no toda infracción procesal es causante de la vulneración del derecho recogido en el arto 24.1 CE, sino que solo alcanza tal relevancia aquella que, por anular las posibilidades de alegación, defensa y prueba cause una verdadera y real situación de indefensión material. El TS[74], siguiendo la citada jurisprudencia de manera inequívoca en numerosas resoluciones, entiende que la tutela judicial exige que la totalidad de las fases del proceso se desarrollen sin mengua del derecho de defensa, y así la indefensión, para cuya prevención se configuran los demás derechos

[72] SSTC 25/2011, Sala 2ª, de 14.03.de 2011 (BOE núm. 86 de 11.04.2011; MP: Elisa Pérez Vera); 164/2005, Sala 2ª, de 20.06.2005 (BOE núm. 173 de 21.07.2005; MP: Eugeni Gay Montalvo); y 185/2003, Sala 1ª, de 27.10.2003 (BOE núm. 283 de 26.11.2003; MP: Pablo García Manzano).

[73] SSTC 126/2011, Sala 2ª, de 18.07.2011 (BOE núm. 197 de 17.08.2011; MP: Francisco Pérez de los Cobos Orihuel); y 122/2007, Sala 2ª, de 21.05.2007 (BOE núm. 149 de 22.06.2007; MP: Vicente Conde Martín de Hijas).

[74] SSTS, Sala 2ª, de 3.12.2015 (ROJ: STS 5100/2015; MP: Andrés Palomo del Arco); 29.10.2015 (ROJ: STS 4677/2015: MP: Francisco Monteverde Ferrer); 27/03/2012 (ROJ: STS 2151/2012; MP: Juan Ramón Berdugo Gómez de la Torre); 13/06/2012 (ROJ: STS 4500/2012; MP: MP: Juan Ramón Berdugo Gómez de la Torre); y 27.09.2011 (ROJ: STS 6068/2011; MP: Francisco Monteverde Ferrer).

instrumentales contenidos en el párrafo 2 del art. 24 CE, se concibe con la negación de la expresada garantía.

Así, resulta conveniente analizar los rasgos de este concepto que la LOPJ convierte en eje nuclear de su normativa. La noción de indefensión, junto con la de finalidad de los actos procesales que se menciona también en el art. 240.1, se convierte en elemento decisivo y trascendental, que cobra singular relieve por su naturaleza y alcance constitucional. Es indudable que el concepto de indefensión comprendido en los arts. 238.3 y 240 LOPJ, ha de integrarse con el mandato del art. 24.1 CE sobre la obligación de proporcionar la tutela judicial efectiva sin que en ningún caso pueda producirse indefensión, aunque ello no signifique en la doctrina constitucional que sean conceptos idénticos o coincidentes. Se ha expuesto, como primero de los rasgos distintivos, la necesidad de que se trate de una efectiva y real privación del derecho de defensa. Es obvio que no basta con la realidad de una infracción procesal para apreciar una situación de indefensión, ni es bastante tampoco con invocarla para que se dé la necesidad de reconocer su existencia. No existe indefensión con relevancia constitucional, ni tampoco con relevancia procesal, cuando aun concurriendo alguna irregularidad, no se llega a producir efectivo y real menoscabo del derecho de defensa con el consiguiente perjuicio real y efectivo para los intereses de la parte afectada, bien porque no existe relación sobre los hechos que se quieran probar y las pruebas rechazadas, o bien, porque resulte acreditado que el interesado, pese al rechazo, pudo proceder a la defensa de sus derechos e intereses legítimos. La indefensión consiste en un impedimento del derecho a alegar y demostrar en el proceso los propios derechos y, en su manifestación más trascendente, es la situación de que el órgano judicial impide a una parte en el proceso el ejercicio del derecho de defensa, privándola de su potestad de alegar y justificar sus derechos e intereses para que le sean reconocidos o para replicar dialécticamente las posiciones contrarias en el ejercicio del indispensable principio de contradicción[75]. No basta, por tanto, con la realidad y presencia de un defecto procesal –cuando existe- si no implica una limitación o menoscabo del derecho de defensa en relación con algún interés de quien lo invoca, sin que le sean equiparables las meras situaciones de expectativa del peligro o riesgo[76]. En definitiva, no son, por lo general, coincidentes de manera absoluta las vulneraciones de normas procesales y la producción de indefensión con relevancia constitucional en cuanto incidente en la vulneración del derecho fundamental a un proceso justo que establece el arto 24 CE.

Por ello la exigencia de que la privación del derecho sea real impone e implica una carga para la parte que la alega, consistente en la necesidad

[75] SSTC 15/1995, Sala 1ª, de 24.01.1995 (BOE núm. 50 de 28.02.1995; MP: Rafael de Mendizábal Allende); 270/1994, Sala 1ª, de 17.10.1994 (BOE núm. 279 de 22.11.1994; MP: Vicente Gimeno Sendra); y 63/1993, Sala 2ª, de 1.03.1993 (BOE núm. 78 de 1.04.1993; MP: Carles Viver Pi-Sunyer).

[76] SSTC 316/1994, Sala 1ª, de 28.11.1994 (BOE núm. 310 de 28.12.1994; MP: Rafael de Mendizábal Allende); y 181/1994, Sala 1ª, de 20.06.1994 (BOE núm. 177 de 26.07.1994; MP: Rafael de Mendizábal Allende).

de proporcionar un razonamiento adecuado sobre tal extremo, argumentando como se habría alterado el resultado del proceso de haberse evitado la infracción denunciada. Ello es así porque la situación de indefensión exige la constatación de su material realidad y no solo de su formal confirmación. Tal exigencia es reiterada de modo constante por la Jurisprudencia del TC[77] y del TS[78] a fin de evitar que bajo la sola invocación de violencias constitucionales se encubra la realidad de meras irregularidades procesales que, encajadas en sede de legalidad ordinaria, no alcanzan cotas de vulneración de derechos reconocidos en la CE.

Por tanto, no bastará con denunciar la ausencia en la correspondiente resolución que autoriza el registro de las condiciones necesarias para asegurar la integridad de los datos volcados de los servidores y dispositivos de almacenamiento informático y de las garantías para preservarlos, sino que será necesario que se especifique el quebranto para el derecho de defensa que del defecto alegado se deriva, o bien expresar o concretar de otro modo la situación de efectiva indefensión resultante. Es evidente que el derecho de defensa no puede verse afectado sin más por la falta de una previa determinación de las precauciones y garantías a adoptar en la toma de datos o en su custodia[79]. Lo relevante es si esas garantías se observaron al realizarse la diligencia y se mantienen tras la recogida de datos con objeto de preservarlos.

5. ACCESO SIN AUTORIZACIÓN JUDICIAL

No siempre que hay afectación de un derecho fundamental es ineludible una habilitación jurisdiccional. Lo que es insoslayable para una intromisión inconsentida del secreto de las comunicaciones o la inviolabilidad domiciliaria –autorización judicial– puede no serlo cuando hablamos solo de intimidad o de privacidad y no de esas manifestaciones específicas[80]. Hay casos en que puede hacerlo la Policía Judicial de propia autoridad. En muchos supuestos, no todos, si concurre un consentimiento libre[81]. En otros, incluso coactivamente[82]. No puede proclamarse precipitadamente el monopolio jurisdiccional como requisito indispensable de toda afectación de un derecho fundamental. La legitimidad constitucional de la detención policial es prueba clara de lo que se afirma. Ni siquiera sería totalmente exacto afirmar que ese es el principio general, solo excepcionado cuando la ley autorice a la policía expresamente.

[77] SSTC 366/1993, Sala 2ª, de 13.12.1993 (BOE núm. 16 de 19.01.1994; MP: José Gabaldón López); y 145/1990, Sala 2ª, de 1.10.1990 (BOE núm. 254 de 23.10.1990; MP: José Gabaldón López).

[78] SSTS, Sala 2ª, de 3.11.2015 (ROJ: STS 4809/2015; MP: Francisco Monteverde Ferrer); 9.12.2014 (ROJ: STS 5068/2014; MP: Juan Ramón Berdugo Gómez de la Torre); y 27.09.2012 (ROJ: STS 6339/2012; MP: Carlos Granados Pérez).

[79] SSTC 290/1993, Sala 1ª, de 4.10.1993 (BOE núm. 268 de 9.11.1993; MP: Miguel Rodríguez-Piñero y Bravo-Ferrer); y 153/1988, Sala 2ª, de 20.07.1988 (BOE núm. 203 de 24.08.1988; MP: Gloria Begué Cantón).

[80] STS, Sala 2ª, de 13.10.2013 (ROJ: STS 5677/2013; MP: Antonio del Moral García).

[81] Por ejemplo, una exploración radiológica.

[82] Cacheos externos.

Actuaciones como la obligación a expulsar unas bolsas de la boca[83] o la toma de huellas dactilares[84] pueden resultar admisibles sin necesidad de una previa validación judicial ni de una ley específica habilitante. Será necesaria la previa intervención judicial cuando la CE o las Leyes así lo exijan. La afectación de un derecho fundamental por sí sola no es argumento siempre suficiente para postular como presupuesto imprescindible la previa autorización judicial salvo explícita habilitación legal[85]. Que una actuación pueda menoscabar la intimidad[86] no significa a priori y como afirmación axiomática que no pueda ser acordada por autoridades diferentes de la jurisdiccional. La jurisdiccionalidad es exigible en algunos casos, en otros, no. Por eso la constatación de la incidencia de la medida en la intimidad no comporta automáticamente previa habilitación judicial inexcusable. No es que se quiera equiparar uno y otro tipo de diligencias. Es obvio que no son equiparables. Esta consideración se hace a los únicos efectos de destacar que no es legal ni constitucionalmente correcta la ecuación afectación de la intimidad–necesidad inexcusable de previa habilitación judicial. 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[87].

En definitiva, a diferencia de lo que sucede con otros derechos, incluido alguno tan significativo, por pertenecer a la misma familia, como el secreto de las comunicaciones o la inviolabilidad del domicilio (art. 18.2 y 3 CE), en los que se reserva enfáticamente al juez la decisión de la interceptación de las comunicaciones o la entrada y registro en domicilio, no se establece ninguna reserva jurisdiccional en favor del derecho a la intimidad personal y familiar (art. 18.1 CE). El TC, sin embargo, hizo extensivo el monopolio del juez al derecho a la intimidad, al menos para las afectaciones que puedan acaecer en el curso de una investigación criminal[88]. La postura de este Tribunal confluye así con la comprensión que las constituciones modernas tienen del poder judicial, del juez, como garante de la libertad, y en tal sentido, como único, o al menos principal, sujeto legitimado para autorizar injerencias de los derechos[89]. La ausencia

[83] STS, Sala 2ª, de 3.07.2007 (ROJ: STS 4993/2007; MP: José Ramón Soriano Soriano).
[84] STS, Sala 2ª, de 21.12.2010 (ROJ: STS 7312/2010; MP: Francisco Monteverde Ferrer).
[85] SSTC 142/2012, Sala 1ª, de 2.07.2012 (BOE núm. 181 de 30.07.2012; MP: Pablo Pérez Tremps); y 206/2007, Sala 1ª, de 24.09.2007, cit.
[86] Por ej. el registro de una maleta o de unos papeles.
[87] La STS, Sala 2ª, de 4.12.2015, cit, aborda un asunto con problemas de acceso a mensajes de correos electrónicos ya recepcionados y guardados en el correspondiente archivo informático.
[88] SSTC 206/2007, Sala 1ª, de 24.09.2007, cit.; 70/2002, Sala 1ª, de 3.04.2002, cit.; y 37/1989, Sala 1ª, de 15.02.1989 (BOE núm. 52 de 2.03.1989; MP: Francisco Rubio Llorente), entre otras muchas.
[89] F. RUBIO LLORENTE, *La forma del poder*, Centro de Estudios Constitucionales, Madrid, 2012, pp. 179 y ss.

constitucional de reserva jurisdiccional facilita, no obstante, que se articulen algunas excepciones a su poder omnímodo. Así, se ha reconocido que el silencio constitucional permite que la ley habilite a la Policía Judicial para realizar aquellas inspecciones o reconocimientos menos invasivos para la intimidad contemplándolo siempre, eso sí, como excepción a la regla general de la preceptiva intervención del juez[90]. Pensemos, con todo, que el TC no se muestra muy proclive a ensanchar el perímetro de las excepciones, pues, aunque admite en términos teóricos la posibilidad de que la Policía Judicial sea autorizada por la ley para que realice determinadas intervenciones leves[91], en la práctica es muy riguroso con los requisitos que ha de reunir a su habilitación legal para que sea considerada legítima, en sintonía con la sólida jurisprudencia del TEDH al respecto[92]. De hecho, el TC tardó en admitir la otra excepción a la autorización judicial previa, que sigue siendo la regla de las limitaciones al derecho a la intimidad personal ex art. 18.1 CE. No fue hasta la STC 70/2002 cuando reconoció que la "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"[93]. La necesidad de una intervención policial inmediata, siempre que a su vez sea proporcionada, es un supuesto habilitante para que la policía adopte medidas que afecten a la intimidad de la persona investigada por la comisión de un delito, sin necesidad de obtener autorización judicial previa[94].

En consonancia con lo expuesto el apartado cuarto del art. 588 sexies c LECRIM regula la posibilidad de acceso directo de la Policía Judicial a la información contenida en los dispositivos de almacenamiento masivo de información, en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. La urgencia alude a una dimensión temporal de la actuación policial que le obligaría a actuar inmediatamente por razones imprescindibles para la prevención y

[90] STC 207/1996, Sala 1ª, de 16.12.1996, cit.
[91] STC 37/1989, Sala 1ª, de 15.02.1989, cit.
[92] STC 207/1996, Sala 1ª, de 16.12.1996, cit.
[93] STC 70/2002, Sala 1ª, de 3.04.2002, cit.
[94] La "acreditadas razones de urgencia y necesidad" y que "se respeten los principios de proporcionalidad y razonabilidad" son a su vez los parámetros que exige el TC para admitir intervenciones sin autorización judicial fuera del ámbito de la investigación criminal, como sucedió en el caso examinado en la STC 233/2005 en que se enjuició, avalándola, una inspección tributaria que se consideraba invasiva de la intimidad de los afectados por haber requerido de sus bancos datos sobre cheques emitidos y destino de las cantidades libradas.

averiguación del delito, el descubrimiento de los delincuentes o la obtención de pruebas incriminatorias[95]. La policía, en otras palabras, sólo está autorizada a intervenir por sí misma, de manera inmediata, sobre el espacio de intimidad de los sospechosos cuando, de no hacerlo, de esperar a la decisión del juez, pueda comprometerse el *ius puniendi* del Estado al frustrarse el buen fin de la investigación penal por la destrucción o por la desaparición de las pruebas, sobre todo si son determinantes, o por la huída a la acción de la Justicia de los posibles sospechosos.

6. CONSENTIMIENTO DEL INTERESADO

El alcance del consentimiento del interesado, cuando de lo que se trata es de aceptar voluntariamente una relación de los mecanismos de exclusión que cada uno de nosotros define frente a terceros y los poderes públicos, ha sido también abordado por la jurisprudencia constitucional[96] recordando 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[97], aunque este consentimiento puede ser revocado en cualquier momento[98]. Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto aún 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[99]. En lo relativo a la forma de prestación del consentimiento el TC[100] ha manifestado que este no precisa ser expreso, admitiéndose también un consentimiento tácito. En suma, la concurrencia del consentimiento de la titular del ordenador excluye la vulneración del derecho a la intimidad[101]. No obstante, es cierto que en la utilización de dispositivos ligados a las nuevas tecnologías convergen distintos derechos no siempre del mismo rango axiológico.

---

[95] SSTC 70/2002, Sala 1ª, de 3.04.2002, cit.; y 207/2007, Sala 1ª, de 16.12.1996, cit.

[96] STC 173/2011, Sala 2ª, de 7.11.2011, cit.

[97] SSTC 196/2006, Sala 1ª, de 3.07.2006 (BOE núm. 185 de 4.08.2006; MP: Jorge Rodríguez-Zapata Pérez); y 83/2002, Sala 1ª, de 22.04.2002 (BOE núm. 122 de 22.04.2002; MP: Pablo García Manzano).

[98] STC 159/2009, Sala 2ª de 29.06.2009, cit.

[99] SSTC 70/2009, Sala 1ª, de 23.03.2009, cit.; y 206/2007, Sala 1ª, de 24.09.2007, cit.

[100] Así, en la STC 196/2004, Sala 1ª, de 15.11.2004, cit., en que se analizaba si un reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, reconoce no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad . También llegan a esta conclusión las SSTC 22/1984, Sala 2ª, de 17.02.1984 (BOE núm. 59 de 9.03.1984; MP: Luis Díez-Picazo y Ponce de León), y 209/2007, Sala 1ª, de 24.09.2007 (BOE núm. 261 de 31.10.2007; MP: María Emilia Casas Baamonde), en supuestos referentes al derecho a la inviolabilidad del domicilio del art. 18.2 CE, manifestando en la primera que este consentimiento no necesita ser expreso y en la segunda que, salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito.

[101] STS, Sala 2ª, de 4.12.2015 (ROJ: STS 5362/2015; MP: Manuel Marchena Gómez).

Se va a citar por su claridad y contundencia la STC 173/2011[102], que recoge un supuesto en el que el recurrente acudió al establecimiento de informática que regentaba el denunciante y le hizo entrega de su ordenador portátil con el encargo de cambiar la grabadora que no funcionaba. El encargado del establecimiento procedió a la reparación tras lo cual, y para comprobar el correcto funcionamiento de las piezas, según el protocolo habitual, eligió al azar diversos archivos para su grabación y posterior reproducción, para lo cual accedió a la carpeta llamada "mis documentos/mis imágenes" del ordenador, encontrando diversos archivos fotográficos de contenido pedófilo que motivaron la interposición de la denuncia. El TC descarta la vulneración del derecho a la intimidad al concurrir consentimiento del afectado que, aunque no autorizó de forma expresa al encargado de la tienda de informática a acceder al contenido de sus archivos o ficheros donde se encontraban las fotografías y videos de contenido pedófilo, sí que es cierto que su conducta no se extralimitó del mandato conferido, añadiendo el Tribunal que avala esta conclusión la circunstancia de que este encargado limitara su actuación a la carpeta "mis documentos" del usuario, mínimo necesario para realizar la referida prueba de grabación, sin pretender adentrarse en otras carpetas respecto de las que, por hallarse más ocultas o por expresarlo así el título asignado a las mismas, pudiera presumirse un mayor revestimiento de protección y reserva. Seguidamente, una vez producido el hallazgo, este se limitó a cumplir con la obligación que le viene legalmente[103] impuesta a todo ciudadano consistente en denunciar ante las autoridades competentes la posible perpetración de un delito público del que ha tenido conocimiento.

Sin embargo, hay autores[104] que han criticado esta conclusión de la referida STC porque no existió un consentimiento del titular que abarcara el examen de los archivos por parte del encargado del establecimiento de informática, ni expreso ni tácito, ni tampoco este le informó previamente sobre la necesidad de examinar archivos para comprobar el funcionamiento adecuado de la grabadora instalada.

La STC comentada consideró que nos encontramos ante uno de los supuestos excepcionados de la regla general, que permite nuestra jurisprudencia, pues existen y pueden constatarse razones para entender que la actuación de la policía era necesaria, resultando, además, la medida de investigación adoptada razonable en términos de proporcionalidad. Razona la citada sentencia que hay que tener en cuenta que la persona denunciada no estaba detenida cuando se practica la intervención, por lo que tampoco aparece como irrazonable intentar evitar la eventualidad de que mediante una conexión a distancia desde otra ubicación se procediese al borrado de los ficheros ilícitos de ese ordenador o que pudiera tener en la "nube" de Internet. Añadiendo que también

[102] STC 173/2011, Sala 2ª, de 7.11.2011, cit.
[103] Arts. 259 y ss. LECRIM.
[104] A. RUIZ LEGAZPI, "Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (*Incoming* de emule) en la STC 173/2011", en *Revista Española de Derecho Constitucional*, núm. 100, 2014, pp. 365-390.

aparece como un interés digno de reseñar la conveniencia de que por parte de los funcionarios policiales se comprobara con la conveniente premura la posibilidad de que existiesen otros participes, máxime en este caso en que se utilizó una aplicación informática que permite el intercambio de archivos, o que, incluso, detrás del material pedófilo descubierto, pudieran esconderse unos abusos a menores que habrían de acreditarse.

La anterior conclusión del TC ha levantado críticas en sectores doctrinales[105] quienes entienden que en el caso abordado por la sentencia no concurría una urgencia y necesidad que legitimara la intervención policial. Hay un voto particular[106] a la sentencia en el que se expresa que no se alcanza a entender por qué, estando el ordenador físicamente en poder de la Policía, las diligencias de investigación no podían esperar a que su realización contara con autorización judicial. Añadiendo que el acceso a archivos de Internet como los que incriminaban al recurrente, sólo puede realizarse si el terminal en cuestión está conectado a la red, por lo que en nada se hubiera puesto en riesgo la labor investigadora de la Policía si, estando dicho terminal en su poder, se mantiene apagado hasta lograr la preceptiva autorización judicial.

Ahora bien, cuestión distinta es el registro del dispositivo realizado directamente por la policía con sustento en el consentimiento del interesado si el mismo está detenido, en cuyo caso será imprescindible que dicho consentimiento se preste en presencia de su abogado, lo que así se hará constar por diligencia policial. El consentimiento a la realización de la diligencia puede afectar, indudablemente al derecho de defensa, por lo que el detenido ha de estar asesorado sobre el contenido y alcance del acto de naturaleza procesal que realiza[107]. Por tanto si el

[105] P. V. CONTRERAS CEREZO, "Internet y la privacidad", en *Diario La Ley*, núm. 7819, 2012, p. 7, afirma que «no puede compartirse la tesis del Alto Tribunal quien justificó la actuación policial, entre otras causas, en una razón de índole técnico, no tomada en cuenta por los tribunales ordinarios, lo que le está vedado, como era la posibilidad de borrado de los archivos a distancia, riesgo que podía ser conjurado, como afirma el voto particular de la sentencia, con un simple apagado del ordenador". R. ALCÁCER GUIRAO, "Derecho a la intimidad, investigación policial y acceso a un ordenador personal", en *La Ley Penal*, núm. 92, 2012, p. 5, entiende que "es discutible que las razones esgrimidas permitan justificar la urgente necesidad de intervención policial y no haber recabado la pertinente autorización judicial, pues en el lapso de tiempo en que el Juez de Instrucción hubiera tardado en pronunciarse no había riesgo alguno de destrucción de pruebas o de comisión de nuevos actos delictivos. En este sentido, podría quizá considerarse proporcionada una intervención policial sobre el ordenador que se hubiera limitado a analizar el contenido de la carpeta «Mis documentos», pudiendo entenderse como la mínima actividad de investigación imprescindible para confirmar la verosimilitud de la denuncia. Pero la garantía derivada del art. 18.1 CE imponía a la Policía el mandato de poner en conocimiento de la autoridad judicial el contenido de esa denuncia y —siendo como era necesaria la medida de acceso al ordenador para la averiguación del delito—, solicitar autorización para ello, por lo que, en definitiva, la actuación policial en el presente caso se reveló desproporcionada y lesiva del derecho fundamental".

[106] Voto particular que formula la Magistrada Elisa Pérez Vera.

[107] SSTS, Sala 2ª, de 10.03.2014 (ROJ: STS 1402/2014; MP: Cándido Conde-Pumpido Tourón); 30.09.2013 (ROJ: STS 4761/2013; MP: Juan Ramón Berdugo Gómez de la Torre); y 2.12.1998 (ROJ: STS 7234/1998; MP: Diego Antonio Ramos Gancedo).

titular está detenido su consentimiento no será válido de carecer al concederlo de asistencia letrada[108]. Si la asistencia de abogado es necesaria para que este preste declaración estando detenido, también le es necesaria para asesorarle si se encuentra en la misma situación para la prestación de dicho consentimiento, justificándose esta doctrina en que no puede considerarse plenamente libre el consentimiento así prestado en atención a lo que se ha venido denominándose "la intimidación ambiental" o "la coacción que la presencia de los agentes de la actividad representan"[109]. Pero existiendo autorización judicial no es preceptiva la presencia de abogado en el momento del registro del dispositivo, sin que se produzca indefensión alguna cuando se ha practicado dándose cumplimiento a los requisitos que de orden constitucional y de legislación ordinaria vienen establecidos[110].

Finalmente destacar que cuando el dispositivo tecnológico incriminatorio lo ocupa un tercero –taxista que encuentra un móvil olvidado en su coche, que resulta poseer pornografía infantil; foro en el que se descubre un participante que emite pornografía infantil, etc.–, la entrega de la evidencia al investigador oficial se equipara, desde el punto de vista del tratamiento probatorio, a la entrega por la víctima, ya que además de que el art. 367 LECRIM excluye tercerías sobre los efectos delictivos sólo interesa atender a la garantía de que la ocupación haya sido hecha de buena fe, evitando las provocaciones delictivas y que se pueda explicar la razón de poseer el dispositivo[111].

7. CONCLUSIONES

1. A pesar de las múltiples funciones tanto de recopilación y almacenamiento de datos como de comunicación con terceros a través de Internet que posee un ordenador personal, el acceso a su contenido podrá afectar bien al derecho a la intimidad personal (art. 18.1 CE), bien al derecho al secreto de las comunicaciones (art. 18.3 CE) en función de si lo que resulta desvelado a terceros son, respectivamente, datos personales o datos relativos a la comunicación. Lo determinante para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE no es el tipo de soporte, físico o electrónico, en el que la información esté alojada ni el hecho, de que el soporte sea un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se

[108]SSTS, Sala 2ª, de 3.04.2001 (ROJ: STS 2769/2001; MP: Juan Saavedra Ruiz); y 23.1.1998 (ROJ: STS 345/1998; MP: José Augusto de Vega Ruiz), entre otras.

[109] SSTS, Sala 2ª, de 17.03.2016 (ROJ: STS 1187/2016; MP: Alberto Gumersindo Jorge Barreiro); 24.02.2015 (ROJ: STS 823/2015; Juan Ramón Berdugo Gómez de la Torre); 23.12.2014 (ROJ: STS 5752/2014; José Ramón Soriano Soriano); y 16.05.2000 (ROJ: STS 3929/2000; MP: Luis Román Puerta Luis), entre otras muchas.

[110] SSTS, Sala 2ª, de 26.04.2012, (ROJ: STS 3027/2012; MP: Cándido Conde-Pumpido Tourón); 27.10.2010 (ROJ: STS 6010/2010; Manuel Marchena Gómez); 23.11.2006 (ROJ: STS 7614/2006; Carlos Granados Pérez).

[111] SAP Guadalajara, Sec. 1ª, de 4.04.2016 (ROJ: SAP GU 134/2016; MP: Isabel Serrano Frías).

accede. Frente a los esfuerzos por diferenciar los derechos fundamentales afectados en función de la naturaleza de cada uno de los contenidos albergados en un ordenador, la jurisprudencia del TS se decanta por una tesis unitaria. La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual.

2. La jurisprudencia del TS ha establecido la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del referido derecho al entorno digital de todo investigado. Esa resolución ha de tener un contenido propio, explicativo de las razones por las que, además de la inviolabilidad domiciliaria, se alza la intimidad reflejada en el ordenador. Nuestro sistema no tolera el sacrificio de los derechos proclamados en los apartados 3 y 4 del art. 18 CE a partir de una legitimación derivada, de suerte que lo que justifica un sacrificio se ensanche hasta validar implícitamente otra restricción. Esta idea tiene ya un reflejo normativo en el art. 588 sexies a) 1º LECRIM. Se trata, por tanto, de una regulación rupturista, que pretende abandonar prácticas en las que la autorización judicial para la entrada en el domicilio del investigado amparaba cualquier otro acto de injerencia, incluso cuando desbordara el contenido material del derecho reconocido en el art. 18.2 CE. Lo que el legislador pretende, por tanto, es que el Juez de instrucción exteriorice de forma fiscalizable las razones que justifican la intromisión en cada uno de los distintos espacios de exclusión que el ciudadano define frente a terceros.

   No ha sido este, sin embargo, el criterio histórico. No pocas resoluciones hacían extensiva la habilitación judicial concedida para la intromisión domiciliaria a la aprehensión de todos aquellos soportes de información que pueda encontrarse en el interior de la vivienda. Sin embargo, el nuevo precepto impide considerar esos instrumentos de almacenamiento como piezas de convicción respecto de las cuales el acceso a su contenido estaría legitimado por la autorización general otorgada por el Juez a los agentes para adentrarse en el domicilio en el que aquéllos son custodiados. El legislador persigue que la restricción constitucional de cada uno de los derechos afectados sea individualmente ponderada por el órgano jurisdiccional, que ha de exteriorizar las razones de su sacrificio. En el plano formal, por supuesto, ningún obstáculo existe para que una misma resolución incorpore el juicio ponderativo del que derivar la legitimidad del sacrificio de los derechos afectados. Para la historia han de quedar las autorizaciones implícitas o sobreentendidas. En definitiva, la entrada y

registro en el domicilio del investigado ha de estar debidamente justificada. El instructor habrá de expresar las razones de la necesidad del sacrificio de ese derecho fundamental. Pero tan argumentado como ese acto de injerencia habrá de estar el acceso a los dispositivos de almacenamiento masivo cuya información resulte indispensable para la investigación.

3. La resolución judicial que autorice el acceso a la información contenida en los dispositivos electrónicos, deberá establecer los términos y el alcance del registro, así como, en su caso, autorizar la realización de copias, fijando las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación. No obstante, la falta de concreción de estos extremos no conllevará la nulidad de la diligencia practicada, por cuanto lo relevante es si esas garantías se observan al realizarse la diligencia y se mantienen tras la recogida de datos con objeto de preservarlos, de forma que la ausencia de tales garantías generen una real y efectiva vulneración del derecho de defensa. En la realización de tales copias, cuando se trate de un clonado o volcado, resulta innecesaria tanto la presencia de fedatario público como la del propio investigado y su abogado. Presencias ambas que sí serán preceptivas cuando se trate de la realización de una copia lógica de archivos.
4. La previsión legal de situaciones de urgencia en lo que se refiere al registro ordinario de equipos informáticos, permitirá el examen directo por la Policía de los datos contenidos en el dispositivo incautado o, en su caso, la ampliación del registro a otros sistemas que resultaran accesibles desde el investigado, siempre que se aprecie un interés constitucionalmente legítimo que haga imprescindible la medida. De la ulterior convalidación judicial de esta actuación policial dependerá la validez de los resultados obtenidos. De manera similar a la interceptación de las comunicaciones telefónicas y telemáticas en supuestos de urgencia se establecen varias reglas: que la información al instructor deberá llevarse a cabo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas; y que en este trámite el sujeto actuante deberá exponer las razones para adoptar esa medida, amén de la actuación llevada a cabo, la forma en que se realizó y su resultado. El juez deberá verificar la concurrrencia de los presupuestos para la adopción de la medida y la justificación de la ejecución anticipada. Tampoco será necesaria autorización judicial cuando el interesado manifieste su consentimiento al registro del dispositivo. Consentimiento que en el supuesto de encontrarse detenido deberá ser prestado a presencia de su abogado so pena de nulidad.

8. BIBLIOGRAFÍA

R. ALCÁCER GUIRAO, "Derecho a la intimidad, investigación policial y acceso a un ordenador personal", en *La Ley Penal*, núm. 92, 2012.

J. A. BONILLA CORREA , "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio (1)", en *Diario La*

Ley, núm. 8522, 20.04.2015.
N. CABEZUDO RODRÍGUEZ, "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", en *Boletín del Ministerio de Justicia*, núm. 2186, 2016.
R. CASANOVA MARTÍN, "Valoración crítica de las intervenciones telefónicas en el borrador de Código Procesal Penal", en V. MORENO CATENA (Dir.) / C. RUIZ LÓPEZ, (Coord.), et. al., *Reflexiones sobre el nuevo proceso penal: Jornadas sobre el borrador del nuevo Código Procesal Penal*, Tirant lo Blanch, Valencia, 2015.
P. V. CONTRERAS CEREZO, "Internet y la privacidad", en *Diario La Ley*, núm. 7819, 2012.
J. DELGADO MARTÍN, "Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos", en *Diario La Ley*, núm. 8202, 29.11. 2013.
J. DELGADO MARTÍN, "La prueba electrónica en el proceso penal", en *Diario La Ley*, núm. 8167, 10.10.2013.
J. F. ETXEBERRÍA GURIDI, "La inadmisibilidad de los tests masivos de ADN en la investigación de los hechos punibles", en *Actualidad Penal*, núm. 28, 1999.
T. FREIXES SAN JUAN, "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos", en Y. GÓMEZ SÁNCHEZ (coord.) / A. TORRES DEL MORAL, et al., *Los Derechos en Europa*, UNED, Madrid, 2001.
M .T. GERALDES DA CUNHA LOPES, "Derecho a la intimidad y la protección de datos en la era de la seguridad global. Principios constitucionales versus riesgos tecnológicos", en *Anuario Jurídico y Económico Escurialense,* núm. 48, 2015.
M. GONZÁLEZ BEILFUSS, El *principio de proporcionalidad en la jurisprudencia del TC*, Aranzadi, Navarra, 2015.
N. GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y derechos fundamentales en el proceso penal*, Colex, Madrid, 1990.
J. L. GONZÁLEZ-MONTES SÁNCHEZ, "Reflexiones sobre el Proyecto de Ley Orgánica de Modificación de la LECRIM para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", en *Revista electrónica de ciencia penal y criminología*, núm. 17, 2015.
A. E. GUDÍN RODRÍGUEZ-MAGARIÑOS, "Incorporación al proceso del material informático intervenido Durante la investigación penal", en *Boletín del Ministerio de Justicia*, núm. 2163, febrero 2014.
M. MARCHENA GÓMEZ / N. GONZÁLEZ-CUÉLLAR SERRANO, *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Castillo de Luna, Madrid, 2015.
A. MARTÍNEZ RETENAGA, *Guía de toma de evidencias en entornos Windows*, Instituto Nacional de Ciberseguidad, Ministerio de Industria, Energía y Turismo, 2014.
E. PEDRAZ PENALVA / V. ORTEGA BENITO, "El principio de proporcionalidad y su configuración en la jurisprudencia del TC y

literatura especializada alemanas", en *Poder Judicial*, núm. 17, 1990.

F. RUBIO LLORENTE, *La forma del poder*, Centro de Estudios Constitucionales, Madrid, 2012.

A. RUIZ LEGAZPI, "Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (Incoming de emule) en la STC 173/2011", en *Revista Española de Derecho Constitucional*, núm. 100, 2014.

C. SANCHÍS CRESPO, "La prueba en soporte electrónico", en E. GAMERO CASADO / J. VALERO TORRIJOS, et al., *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*. Aranzadi, Navarra, 2012.

P. SANTOLAYA MACHETTI, "Limitación a la aplicación de las restricciones de derechos: un genérico límite a los límites según su finalidad", en J. GARCÍA ROCA / P. SANTOLAYA MACHETTI (Coords.), et al., *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2005.

E. VELASCO NÚÑEZ, "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", en *Diario La Ley*, núm. 8183, 4.11.2013.