DERECHO A LA INTIMIDAD Y REGISTRO DE DISPOSITIVOS INFORMÁTICOS: A PROPÓSITO DEL ASUNTO *TRABAJO RUEDA C. ESPAÑA*[1]

The right to privacy and the registration of computer devices: About case of *Trabajo Rueda v. Spain*

JUAN OCÓN
Universidad de La Rioja
juan.ocon@unirioja.es

Cómo citar/Citation
Ocón, J. (2018).
Derecho a la intimidad y registro de dispositivos informáticos:
a propósito del asunto *Trabajo Rueda c. España.*
Revista Española de Derecho Constitucional, 113, 327-343.
doi: https://doi.org/10.18042/cepc/redc.113.11

Resumen

La Ley Orgánica 13/2015 introdujo en nuestro ordenamiento la regulación de las diligencias de investigación tecnológicas. Con anterioridad, fueron los tribunales los encargados de dar respuesta al registro policial del contenido de un ordenador sin previa autorización judicial y su incidencia en el derecho a la intimidad. Este es el problema suscitado en el asunto *Trabajo Rueda c. España*, de cuyo estudio se ocupa el presente artículo.

Palabras clave

Intimidad; nuevas tecnologías; registro de ordenadores; garantía de los derechos fundamentales.

[1] Este trabajo ha sido elaborado al amparo del Proyecto DER2014-52817-P, MINECO. Agradezco la labor realizada por los evaluadores, que han mejorado estas páginas con sus acertadas aportaciones.

Abstract

Organic law 13/2015 introduced into our legal system the technological investigation measures. Previously, courts of Justice were responsible for responding to the police record of the contents of a computer without prior judicial authorization and its impact on the right to privacy. This is the problem raised in the case of *Trabajo Rueda v. Spain*, whose subject is dealt with in this paper.

Keywords

Privacy; new technologies; registration of computer devices; guarantee of fundamental rights.

SUMARIO

I. INTRODUCCIÓN

Que la realidad va siempre por delante del derecho es una afirmación incuestionable si los términos en comparación son, por un lado, una decimonónica Ley de Enjuiciamiento Criminal y, por otro, el uso de las nuevas tecnologías en la investigación de las conductas aparentemente delictivas.

Y es que la regulación de las medidas de investigación tecnológicas no se plasma en nuestro derecho hasta la aprobación de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Con el código procesal penal en un horizonte impreciso —si consideramos que se han conocido dos borradores de proyecto en los últimos años—, el legislador se ha decidido a introducir en la nueva norma cuestiones que no pueden esperar a la aprobación de aquel y que, hasta este momento, han sido resueltas con desigual fortuna mediante decisiones jurisprudenciales.

Ese notable material jurisprudencial constituía sin duda «una fuente privilegiada de soluciones normativas» (Marchena Gómez, 2013: 5)[2]. No obstante, y aun pudiendo considerarse suficiente tal acervo jurisprudencial para superar los escrutinios del TEDH[3], no parece esta una solución permanente y

[2] Los criterios y principios establecidos en la jurisprudencia previa se acogen de plano ahora en la norma, tal y como reitera repetidamente el apdo. IV del preámbulo de la LO 13/2015.

[3] En el ámbito del Convenio, el TEDH ha entendido el término ley en su acepción material y no formal, incluyendo, por tanto, la jurisprudencia. Por todas, STEDH *Sunday Times c. Reino Unido*, de 26 de abril de 1979, párr. 47: «The Court observes that the word `law´ in the expression `prescribed by law´ covers not only statute but also unwritten law».

fiable capaz de responder a las garantías exigibles a un Estado de derecho cuando se trata de limitar derechos fundamentales.

En este estado de la regulación nacional española, el TEDH entiende, en el asunto *Trabajo Rueda c. España* (32600/12), a cuyo análisis se presta el presente artículo, de la conformidad con el Convenio del acto de registro policial de un ordenador personal sin disponer de autorización judicial previa.

Comenzaremos ofreciendo algunas apreciaciones sobre el derecho fundamental en juego, destacando algunos aspectos del *iter* judicial para desembocar finalmente en el análisis de la regulación vigente que propone la LO 13/2015 para el supuesto de la actuación sometida a enjuiciamiento ante el TEDH en *Trabajo Rueda*.

II. ALGUNAS NOTAS SOBRE EL DERECHO FUNDAMENTAL A LA INTIMIDAD

En el proceso, la actuación policial se ha confrontado con una eventual vulneración del derecho a la intimidad del art. 18.1 CE.

Los derechos del art. 18 CE tienen como objetivo común principal el de otorgar protección a determinados aspectos de la vida privada —la intimidad, el domicilio, las comunicaciones—, es decir, aquello que no es, o que no queremos que sea, de general conocimiento. Dentro, y como parte de ello, se contiene un núcleo que entendemos como esencial en la autoconciencia personal: es a esto a lo que denominamos intimidad.

El derecho fundamental a la intimidad pretende garantizar al individuo un ámbito reservado frente a la acción y conocimiento de los demás. De esta manera, «lo que el art. 18.1 CE garantiza es, pues, el secreto sobre nuestra propia esfera de la vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los contornos de nuestra vida privada»[4].

La característica de este derecho se cifra en la delimitación de su objeto, dado que es el propio titular el apoderado por el ordenamiento para configurarlo[5].

Como es sabido, la postura inicial de nuestro Tribunal Constitucional fue la de seguir un criterio material para definir la «esfera privada», esto es, será privado aquello que, según las pautas sociales imperantes, suele considerarse

[4] STC 85/2003, de 8 de mayo (FJ 21).

[5] «Lo que para una persona puede ser susceptible de la reserva más extrema, para otra puede ser un orgullo su conocimiento» (Zoco Zabala, 2015: 99).

reservado o ajeno al legítimo interés de los demás (Díez-Picazo Giménez, 2008: 299)[6]. En este sentido se expresa la STC 231/1988, de 2 de diciembre (FJ 3), al reconocer que:

> Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 de la C.E. aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la «dignidad de la persona», que reconoce el art. 10 de la CE, y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana.

No obstante, según sabemos, desde finales de los años noventa la jurisprudencia constitucional ha utilizado en ocasiones una visión formal o subjetiva, al reconocer que «corresponde a cada persona acotar el ámbito de la intimidad personal y familiar que reserva al conocimiento ajeno»[7].

En todo caso, el registro de dispositivos informáticos en el marco del proceso penal de que nos ocupamos presenta una característica especialmente reseñable: a diferencia de lo previsto para la inviolabilidad del domicilio o para el secreto de las comunicaciones, el art. 18.1 CE no prevé que el derecho a la intimidad pueda ser delimitado restrictivamente mediante resolución judicial[8].

---

6 Puede que el término «esfera privada» no sea el más adecuado, por cuanto que nuestra Constitución no reconoce, como sí lo hacen otros textos, el derecho a la vida privada. Aunque, como se ha dicho, de haberse reconocido cabría entender como manifestaciones de aquel el honor, la intimidad y la propia imagen, lo cierto es que el art. 18.1 CE configura tres derechos distintos y autónomos (Rebollo Delgado, 2005: 191). No obstante, estos derechos se encuentran estrechamente vinculados entre sí, por lo que en ocasiones se alegan varios de ellos en amparo. Ahí puede hallarse la excusa para acudir a la «esfera privada» como concepto más amplio que los albergue. En todo caso, consideramos que rebosa, por su carácter ilimitado, incluso la suma de los objetos —limitados— de los tres derechos reconocidos.

7 STC 196/2006, de 3 de julio (FJ 5). Esta postura ha sido criticada por parte de la doctrina al entender que puede suponer un riesgo tanto desde el punto de vista positivo —libertad del individuo para renunciar a su intimidad— como negativo —posibilidad de excluir del conocimiento ajeno aquellos aspectos de incuestionable interés público—. Véase Díez-Picazo Giménez (2008: 299 y ss.). Sobre la evolución de la jurisprudencia constitucional puede verse Martínez de Pisón Cavero (2016).

8 Entendemos que, en el caso que aquí nos ocupa, la resolución judicial que autoriza el registro de un ordenador personal no se dirige a restringir *per se* el derecho a la intimidad, sino que simplemente permite llevar a cabo una medida potencialmente

Sin embargo, el TC ha entendido, con base en la idea de que no existen derechos fundamentales ilimitados o absolutos, que el derecho a la intimidad puede verse sometido a restricciones ante ciertas «exigencias públicas» y bajo el cumplimiento de determinadas condiciones[9].

La justificación objetiva y razonable de esa restricción pasaría, según nuestro TC, por apreciar los siguientes requisitos:

> […] la existencia de un fin constitucionalmente legítimo […]; que la medida limitativa del derecho esté prevista en la ley (principio de legalidad); que como regla general se acuerde mediante una resolución judicial motivada (si bien reconociendo que debido a la falta de reserva constitucional a favor del Juez, la Ley puede autorizar a la policía judicial para la práctica de inspecciones, reconocimientos e incluso de intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad) y, finalmente, la estricta observancia del principio de proporcionalidad, concretado en tres requisitos o condiciones: idoneidad de la medida, necesidad de la misma y proporcionalidad en sentido estricto[10].

De entre ellos, y por lo que aquí interesa, cobra especial importancia —por su inobservancia en el asunto analizado— la necesidad de resolución judicial. La jurisprudencia constitucional ha permitido excepcionar la regla general en los casos en que, además de respetar el principio de proporcionalidad, «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», debiendo valorar *ex ante* la urgencia y necesidad[11].

---

vulneradora en el derecho fundamental considerado. Dado el carácter material del derecho fundamental a la intimidad, la injerencia dependerá del contenido que albergue el dispositivo registrado y, por tanto, la vulneración o no en la intimidad de su propietario solo se conocerá una vez efectuado el registro. Consideramos que la estructura es entonces similar a la prevista en el art. 18.3 CE: la autorización judicial para delimitar restrictivamente el derecho se produce con independencia y con absoluto desconocimiento del contenido de la comunicación que va a ser intervenida. Por tanto, la autorización judicial se requiere no ya porque la medida se proyecte necesariamente y en todo caso sobre la intimidad, sino porque el registro se lleva a cabo sobre un escenario idóneo —en este caso un dispositivo informático, en otros una comunicación o el domicilio— para vulnerar esa intimidad.

9 STC 37/1989, de 15 de febrero, FJ 7. Véase Subijana Zunzunegui (1997).

10 Por todas: STC 70/2002, de 3 de abril (FJ 10).

11 *Ibid*.

Es evidente que en los dispositivos informáticos —por ejemplo, un ordenador o un *smartphone* de uso personal— pueden acumularse contenidos amparables por el art. 18 CE. Lo problemático es determinar qué derecho de los allí recogidos se pone en juego con ocasión de su registro. De ahí que determinadas resoluciones judiciales hayan tratado de proponer una respuesta integral de los derechos apuntados, sugiriendo un derecho autónomo al propio entorno virtual o digital.

De esta manera, la STS de 17 de abril de 2013 (FJ 8) reconoce que «en el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE)», pero también «información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones».

Por ello, considera que «la ponderación judicial de las razones que justifican […] 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», y afirma en consecuencia que «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».

En esa línea, entiende 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 el que se integraría] 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»[12].

Más allá de la opinión que puedan merecer estas resoluciones, la solución a la que llega la actual regulación es en cierto modo coincidente con esa propuesta de tratamiento unitario, pues, tras rubricar el título VIII LECrim como «De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución», no individualiza los derechos afectados por cada una de las medidas reguladas al establecer unas disposiciones comunes a todas las diligencias tecnológicas de investigación[13].

---

[12] Esta tesis ha sido mantenida por resoluciones posteriores: así, entre otras, las SSTS de 18 de julio de 2014 (FJ 4), de 24 de febrero de 2015 y de 4 de diciembre de 2015. Se ha situado el origen de ese supuesto «derecho al entorno virtual propio» en la Sentencia del Tribunal Constitucional Federal Alemán de 27 de febrero de 2008 (Bachmaier Winter, 2017: 21).

[13] Véase *infra* apartado IV.

III. *ITER* PROCESAL DEL ASUNTO *TRABAJO RUEDA*

1. LOS HECHOS

El señor Trabajo Rueda acudió a un establecimiento dedicado a servicios de reparación informática con el objetivo de que sustituyeran la unidad grabadora de su ordenador personal, sin que el acceso a tal dispositivo estuviese protegido por contraseña u otro sistema.

Realizado el trabajo encargado, el técnico, siguiendo la práctica habitual —según él mismo relata—, accedió a la carpeta «Mis documentos/Mis archivos» con el fin de reproducir algún archivo de cierto volumen y comprobar, con ello, el resultado de la reparación.

Es entonces cuando el técnico visualiza que el dispositivo alberga diversas imágenes pornográficas de menores, procediendo a dar cuenta de su hallazgo a la policía, facilitando los datos identificativos del señor Trabajo Rueda y reconociéndole fotográficamente en comisaría.

El 18 de diciembre de 2007 la policía accede a la carpeta señalada por el técnico denunciante, pero también a la denominada «Incoming», en la que por defecto se almacenan los archivos descargados del programa eMule —que estaba configurado para compartir con el resto de usuarios los archivos almacenados en su disco duro—, donde también hallan un gran volumen de material pedófilo.

El día siguiente es detenido el señor Trabajo Rueda y, tras tomarle declaración en comisaría, se remite el ordenador al grupo de pericias informáticas de la brigada provincial de policía judicial para que realizase un examen exhaustivo del contenido.

El día 20 el detenido pasa a disposición del juez de instrucción, quien, tras incoar diligencias previas, toma declaración al agente que había instruido el atestado policial.

2. LA JURISDICCIÓN ORDINARIA

En atención a lo anterior, el señor Trabajo Rueda es acusado y condenado como autor por un delito de corrupción de menores previsto y penado en el art. 189, apdos. 1.b) y 3.a) del Código Penal en su redacción vigente al momento de la comisión de los hechos[14].

[14] El art. 189.1.b) disponía que: «Será castigado con la pena de prisión de uno a cuatro años: […] b) El que produjere, vendiere, distribuyere, exhibiere o facilitare la

Tanto en la sentencia de instancia —SAP de Sevilla, sección 1.ª, de 7 de mayo de 2008— como en el recurso de casación —STS, Sala de lo Penal, de 18 de febrero de 2009—, la defensa del señor Trabajo Rueda denuncia que el acceso al contenido de su ordenador, tanto por el técnico como por la policía, se había producido sin contar ni con la autorización del titular, ni con la debida resolución judicial que acordase la medida, entendiendo por tanto que se había producido una lesión de su derecho fundamental a la intimidad (art. 18.1 CE)[15].

Ambas resoluciones, coincidentes en el núcleo de su argumentación, entienden incólume el derecho fundamental a la intimidad del señor Trabajo Rueda. Para llegar a tal conclusión no entran a valorar la doctrina constitucional sobre el derecho considerado, ni plantean siquiera la existencia de circunstancias que permitan excepcionar la necesidad de autorización judicial. Resuelven el asunto entendiendo que existe una suerte de autorización tácita por parte del acusado que basan en dos aspectos: por un lado, la inexistencia de contraseña en el dispositivo y el hecho de que no se pusieran límites al técnico en el uso del ordenador y, por otro lado, la configuración «abierta» del programa eMule.

Pueden hallarse fácilmente objeciones a la argumentación expuesta, coincidentes con las alegadas en amparo: la ausencia de autorización del propietario para acceder al ordenador a los agentes de policía o la ignorancia previa a la inmisión de la configuración «abierta» para el acceso *on line* al contenido por terceros.

producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido». Por su parte, el apdo. 3.a) regulaba el subtipo agravado, previendo una pena de prisión de cuatro a ocho años cuando concurriese, entre otras circunstancias, la de utilizar a menores de 13 años. Nótese que tal calificación se produce por la configuración del programa eMule en el dispositivo del acusado, ya que permitía compartir sus archivos con otros usuarios y, por tanto, la conducta es subsumible en la acción de distribución. De tomar en cuenta solamente los archivos hallados por el denunciante en la carpeta «Mis documentos» estaríamos ante un delito de posesión de pornografía infantil, castigado con pena de tres meses a un año de prisión o con multa de seis meses a dos años.

15 La consecuencia de admitir la vulneración alegada debía ser la nulidad de la prueba así obtenida, por cuanto que el art. 11.1 LOPJ dispone que: «No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales». En casación se alega también como motivo la vulneración del art. 24.2 CE por entender que todo el material probatorio de la instancia es nulo por basarse en la pericial informática.

3. LA SENTENCIA DE AMPARO

El asunto llega al Tribunal Constitucional mediante la interposición de un recurso de amparo en el que se alega una supuesta vulneración de los derechos a un proceso con todas las garantías, a la presunción de inocencia y, en lo que interesa al presente trabajo, a la intimidad.

El recurso es resuelto por la STC 173/2011, de 7 de noviembre de 2011 —que cuenta con un voto particular de la magistrada Elisa Pérez Vera—, en una resolución cuya argumentación parece derivar al otorgamiento del amparo hasta el fundamento jurídico 7, donde considera que la actuación tiene cabida en los supuestos excepcionales de exención de autorización judicial[16].

El Tribunal realiza un recorrido por su doctrina sobre el derecho fundamental considerado (FJ 2). Recuerda la posibilidad de incidir en el mismo, bien cuando exista consentimiento eficaz de su titular, bien ante la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos. Como dijimos, en este segundo escenario se requiere, además, la previsión legal de la autorización judicial —aunque con la posibilidad de obviarla en determinados supuestos— y el estricto cumplimiento del principio de proporcionalidad.

Pues bien, en estas dos posibilidades de incidir en la intimidad el Tribunal va a encontrar acomodo tanto a la actuación del denunciante como a la de la policía.

Entiende que la actuación del señor Trabajo Rueda encierra «una declaración expresiva de su voluntad de hacer entrega a dicho encargado de su portátil, poniéndolo a su disposición, para que éste procediera a su reparación», por lo que considera que el técnico se encontraba amparado en su proceder por la autorización expresa del titular y, por tanto, no habiéndose extralimitado del mandado recibido, no puede entenderse vulnerado el derecho a la intimidad del condenado (FJ 5).

Sin embargo, frente a la posición de la Audiencia y el TS, niega que aquella autorización pueda prolongarse a la policía, pues solo la violación de la intimidad permitiría acceder a una justificación de la invasión (FJ 6).

El Tribunal pasa a analizar la actuación policial invasiva a la luz del resto de los presupuestos habilitantes enumerados *supra* (FJ 7).

La obviedad de la tesitura permite al Tribunal acreditar la concurrencia de un fin constitucionalmente legítimo en «el interés público propio de la investigación de un delito».

[16] Puede encontrarse un excelente análisis de esta sentencia, y premonitorio de la resolución del TEDH en Ruiz Legazpi (2014).

Pero parece igualmente obvio que nuestro ordenamiento no contempla una previsión legal para esta medida.

En ausencia de una regulación específica, el Tribunal entiende amparada la actuación policial en una serie de normas generales que facultan a la policía judicial para la práctica de diligencias dirigidas a investigar delitos y descubrir a los delincuentes[17]. El problema, como apunta acertadamente el voto particular, reside en que la normativa considerada autoriza a los agentes para efectuar un «primer análisis» de los efectos intervenidos, lo que difícilmente comulga con que, con esta sola y genérica habilitación, pudiera accederse, ilimitada y minuciosamente, a todo el contenido del artificio electrónico.

Considera el TC, además, que la necesidad de la medida llevada a cabo por la policía hace que pueda clasificarse dentro de la excepción permitida a la regla general de autorización judicial previa[18].

Pero donde la deferencia hacia la justicia ordinaria rebasa lo razonable es en la aceptación como argumentos de dos consideraciones que no debieran de haber rebasado las fronteras de las fuerzas de seguridad e invadir el cuerpo de la decisión jurisdiccional. En primer lugar, la celeridad necesaria para comprobar la veracidad de los hechos denunciados, teniendo en cuenta, además, la gravedad de estar ante un delito de distribución de pornografía infantil. En segundo lugar, la necesidad de asegurar las pruebas ante la posibilidad de que

---

17 El TC ha apuntado la existencia de «la triple condición que exige nuestra Constitución sobre la previsión legal de las medidas limitadoras de derechos fundamentales: la existencia de una disposición jurídica que habilite a la autoridad judicial para la imposición de la medida en el caso concreto, el rango legal que ha de tener dicha disposición, y la calidad de Ley como garantía de seguridad jurídica», STC 169/2001, de 16 de julio. Si bien, como veremos, el requisito de calidad de la ley en términos de precisión, calidad y previsibilidad puede ser salvado en el ámbito del Convenio con base en su concepto material de ley, mayores dudas plantea en nuestro sistema constitucional, como así se apunta en el voto particular formulado a la sentencia analizada. Consideramos que esa intervención del legislador debe ser particularmente necesaria y especialmente cuidadosa en el ámbito del proceso penal por la potencialidad lesiva que en ese escenario se produce para los derechos fundamentales.

18 Resulta ilustrativo que, pese a que en el FJ 2 el Tribunal había dicho —recordando su doctrina— que en caso de actuar sin autorización judicial deben «acreditarse razones de urgencia y necesidad que hagan imprescindible la actuación inmediata», a la hora de valorar precisamente la ausencia de dicha autorización ni siquiera nombre —tal vez consciente de la dificultad de su acreditación— el concepto de «urgencia».

se produjese un borrado de los ficheros ilícitos «mediante una conexión a distancia desde otra ubicación»[19].

Estamos ante un caso de cesión ante el argumento general de la eficacia de las fuerzas policiales que, en este supuesto, es inconsistente y falaz.

En primer lugar, porque la gravedad de la modalidad delictiva se conoce precisamente mediante la actuación policial sospechosa de irregular.[20] En segundo lugar, porque estando el ordenador físicamente en manos de la unidad de delitos informáticos de la policía, todo indica que difícilmente se mantendría conectado a red, siendo imposible así eliminar archivos de forma remota[21].

En fin, el Tribunal logra así finalmente superar todos los obstáculos para acreditar una actuación policial respetuosa con el principio de proporcionalidad en sus tres dimensiones: idoneidad, necesidad y proporcionalidad en sentido estricto. Y, por tanto, con el ordenamiento jurídico. Cabe, pues, sacrificio del derecho fundamental a la intimidad. Y denegación del amparo.

4. LA SENTENCIA DEL TEDH

El TEDH, en sentencia de 30 de mayo de 2017, tras desestimar los motivos de oposición planteados por el Gobierno[22] y admitir a trámite el recurso (párrs. 25 y ss.), consideró que la actuación de las autoridades públicas, consistente en acceder a los archivos del ordenador, supuso una injerencia en la privacidad del demandante.

---

[19] Consideramos que el manejo de los conceptos que el TC realiza en la argumentación que ofrece en este FJ 7 no es muy afortunado ya que, pese a apuntar que «la actuación de la policía era necesaria» —lo que llevaría a valorar la inexistencia de otras medidas menos gravosas—, los motivos que ofrece para sostener esa afirmación obedecen a una justificación, por un lado, de la proporcionalidad en sentido estricto (gravedad del delito) y, por otro, de la urgencia (asegurar las pruebas).

[20] Nótese que la intromisión ilimitada es la que permite averiguar la existencia de un tipo de delito agravado, frente al delito menos grave deducible del reconocimiento preliminar. Es la invasión exorbitante la que termina siendo corregida por el resultado obtenido: una inquietante práctica; y contundentemente rechazable.

[21] En el mismo sentido, Ruiz Legazpi (2014: 389).

[22] Alega el Gobierno, entre otros motivos de inadmisión, que el señor Trabajo Rueda no había sufrido daño alguno, por cuanto se sustrajo de la justicia hasta que se declaró la prescripción de la responsabilidad penal. Para el TEDH, el solo hecho de haber sido condenado a una pena de prisión con base en una presunta vulneración del derecho a la vida privada debe considerarse «perjuicio importante» a los efectos del art. 35.3.b) CEDH.

La legitimidad de esa injerencia dependerá de la concurrencia de los requisitos establecidos en el segundo párrafo del art. 8 del Convenio, para cuyo análisis deberá someterse a la medida a un triple examen: el de su previsión legal, su finalidad legítima y su necesidad en una sociedad democrática.

a) Una injerencia prevista por la ley (párrs. 33 a 38).
   El TEDH comienza por constatar la inexistencia de normativa reguladora del acceso por parte de los poderes públicos al contenido de dispositivos informáticos. Declara igualmente la insuficiencia de las normas genéricas reguladoras de la actuación policial en la investigación de delitos. Pasa por tanto a evaluar la existencia de la jurisprudencia constitucional existente al momento de producirse la injerencia denunciada.
   El TEDH se hace eco de los problemas que pueden derivarse de la posibilidad jurisprudencialmente prevista de excepcionar la autorización judicial en casos de «urgencia» o «urgente necesidad». No obstante, entiende que la posibilidad de control judicial posterior de tan imprecisa cláusula, que permite por tanto a la justicia realizar un escrutinio de la corrección del procedimiento de obtención de pruebas incriminatorias, supone una garantía suficiente frente a una eventual arbitrariedad.
   Por tanto, el TEDH considera que existe una previsión legal «material» de base jurisprudencial suficientemente clara y precisa.
b) Una injerencia que persigue un fin legítimo (párrs. 39 a 41).
   El Tribunal de Estrasburgo declara que la actuación de la policía estaba orientada al cumplimiento de fines legítimos previstos en el Convenio, señaladamente los de «prevención de las infracciones penales» y «protección de los derechos y las libertades de los demás».
c) Una injerencia necesaria en una sociedad democrática (párrs. 42 a 48).
   El Tribunal recuerda su doctrina constante. La valoración de la medida requiere atender a su «necesidad social imperiosa», a su proporcionalidad respecto del fin perseguido y a la pertinencia y suficiencia de los motivos invocados por las autoridades nacionales para justificarla.

En atención a ello, considera que los agentes se extralimitaron al inspeccionar contenidos del ordenador «más allá» del directorio informático genérico normalmente, y también en este caso concreto, denominado «Mis documentos», pues no disponía de habilitación para tan ilimitada invasión.

Al carecer de autorización judicial, el registro resistía el escrutinio de proporcionalidad con base en una «urgente necesidad» para la que el TEDH no encuentra justificación en el caso concreto. Y ello porque no existía riesgo de

daño o pérdida de los archivos, ni cabía el acceso de terceros al dispositivo informático a fin de destruir o alterar las pruebas incriminatorias que pudiere contener.

La medida es declarada desproporcionada e innecesaria.

Por lo que se refiere a las consecuencias de la vulneración declarada, y pese a la solicitud del señor Trabajo Rueda[23], el TEDH considera que la constatación de la violación constituye en sí misma una reparación suficiente del daño sufrido por el titular del derecho.

IV. LA ACTUAL REGULACIÓN DEL REGISTRO DE DISPOSITIVOS DE ALMACENAMIENTO MASIVO

La situación normativa existente al momento de producirse los hechos, caracterizada por la ausencia de una regulación específica de las medidas de investigación tecnológicas, cambia con la modificación que en la LECrim lleva a cabo la Ley Orgánica 13/2015.

Entre otras, configura de forma autónoma la diligencia controvertida en el caso analizado[24]. La norma vigente permite acceder, en el marco de una investigación penal, al contenido de ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento masivo de información digital o repositorios telemáticos de datos.

Por tanto, parece oportuno exponer los criterios y requisitos que establece para efectuar un registro de un ordenador personal y confrontarlos con la actuación policial enjuiciada.

La ley parte de la diferenciación entre la mera aprehensión de los dispositivos y la posibilidad, esta sí relevante, de acceder a la información que en ellos se contiene, para lo que exige autorización judicial específica[25].

---

[23] Reclamaba una indemnización de 134 805 euros por los perjuicios que le había producido vivir en la clandestinidad para no cumplir la condena.

[24] Esta diligencia de investigación, al igual que otras que se prevén ahora en la norma, se proyecta sobre dispositivos que albergan contenidos y datos que, en principio, son objeto de una diferente protección iusfundamental. Sin embargo, la norma no tiene en cuenta esta diversidad de regímenes de protección constitucional y establece una regulación común a partir de la rúbrica de su título VIII como «De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución», no atendiendo, por tanto, a los diferentes objetos de los derechos fundamentales protegidos en el artículo citado.

[25] Tanto el contenido de la resolución judicial como los principios que debe valorar el juez a la hora de autorizar la medida se regulan de forma conjunta para todas las diligencias de investigación tecnológicas en los arts. 588 bis.a*)* a 588 bis.k*)*.

La norma contempla la posibilidad de que los dispositivos puedan ser incautados tanto dentro del domicilio —art. 588 sexies.a— como fuera del mismo —art. 588 sexies.b—, pero condicionando en ambos casos la legitimidad de acceder a la información que albergan a la existencia de una previa autorización judicial.

Para el segundo supuesto —que es el que se produce en el caso analizado—, la ley ordena a los agentes de policía dar cuenta al juez de instrucción de la incautación del dispositivo, a quien corresponde autorizar el acceso a su contenido si lo considera indispensable para el buen fin de la investigación.

En cualquier caso, en la resolución debe determinarse tanto el alcance del registro como las condiciones llamadas a asegurar la intangibilidad e integridad de la información obtenida[26].

Se prevé también la posibilidad de suspender en el tiempo la garantía judicial, atendiendo a razones de urgencia y tratando de evitar que pueda verse frustrada la investigación.

En ese caso, la medida puede ser directamente llevada a cabo por la unidad policial encargada de su ejecución (art. 588 sexies.c.4), debiendo informar al juez acerca de la justificación, extensión y resultados de la medida lo antes posible y siempre en el plazo improrrogable de veinticuatro horas. Por su parte, el órgano judicial deberá confirmar o revocar de forma motivada la pertinencia de la medida en el plazo máximo de 72 horas. La revocación de la medida deberá conllevar, como es lógico, la exclusión de la causa de la información obtenida con su ejecución.

A diferencia de lo previsto para otras medidas, no contiene la norma un catálogo de delitos para cuya investigación pueda acordarse esta diligencia, lo que no libera al órgano judicial de tener que aplicar estrictamente los principios de idoneidad, necesidad y proporcionalidad en sentido estricto, y con especial celo por hallarnos ante una medida con tan alto grado de afección en la esfera de la privacidad del investigado.

En atención a lo expuesto, puede concluirse que los criterios establecidos en la jurisprudencia para acceder al contenido de dispositivos informáticos en ausencia de regulación son coincidentes con los ahora previstos legalmente[27].

---

[26] Se han puesto en duda estas garantías por la imperfección de la regulación ofrecida desde un punto de vista informático, apuntando a una falta de esfuerzo de la ley por evitar algo con tan altas posibilidades como la manipulación de los dispositivos electrónicos. Véase Rubio Alamillo (2015).

[27] No se prevé legalmente, sin embargo, la posibilidad de que el registro se legitime por el consentimiento del titular del dispositivo, aunque entendemos que debe considerarse plenamente válido.

Por tanto, la legitimidad de un registro policial sin autorización judicial —como el llevado a cabo en el asunto estudiado— depende también ahora de la valoración que se haga de la concurrencia de la urgente necesidad como criterio que puede excepcionar aquella, por lo que, en este sentido, la resolución sería similar[28].

No existe, ni en la norma ni en la jurisprudencia constitucional, una lista de criterios objetivos para establecer qué debe entenderse por «urgente necesidad». En todo caso, podemos extraer algunos de esos criterios de los pronunciamientos de nuestro Tribunal Constitucional; a saber: riesgo de desaparición de las pruebas, posibilidad de que el presunto autor se sustraiga de la justicia, extensión de los efectos del delito o comisión de otros, o la imposibilidad o dificultad de poner en conocimiento inmediato de la autoridad judicial las actuaciones practicadas.

En este sentido, la STC 115/2013, de 9 de mayo (FJ 6), considera probada la urgencia en el acceso policial a la agenda de un teléfono móvil que los agentes encontraron encendido en el lugar de los hechos, donde sorprendieron al recurrente custodiando un importante alijo de droga. En opinión del Tribunal se justifica la urgencia en la identificación de los presuntos autores a través del acceso a la agenda del terminal a fin de evitar que se sustrajeran definitivamente a la acción de la justicia. Razones de urgencia y necesidad que se ven reforzadas, dice el TC, por la flagrancia del delito.

Por lo dicho hasta ahora consideramos que, si bien puede ser necesaria la actuación policial sin autorización judicial en determinadas situaciones, tal posibilidad debe ser sometida necesariamente a un férreo y riguroso control judicial posterior que le confiera la legitimidad exigible en un sistema garantista de derechos fundamentales.

En la mayoría de los supuestos, la vulneración denunciada se produce con el material probatorio (ordenador, teléfono móvil) ya en manos de los agentes de policía. Entendemos que en estos casos podría ser plausible, a la hora de examinar la concurrencia de la urgencia, comparar los riesgos de la no actuación inmediata frente a la alternativa de acudir a los actuales servicios judiciales de guardia para conseguir la resolución habilitante.

Sin embargo, no encontramos en las resoluciones analizadas grandes construcciones argumentativas a la hora de justificar la concurrencia de esa urgencia que permitiría suspender en el tiempo la garantía judicial y calificar la actuación como «necesaria en una sociedad democrática».

---

[28] No obstante, la ley establece para estos casos unos plazos que en el asunto *Trabajo Rueda* no fueron cumplidos, debiendo, por tanto, anularse las pruebas ilegalmente obtenidas.

Parece que, pese a que se prevén ahora legalmente los criterios de injerencia en el derecho considerado, la reforma no ha reducido la incertidumbre en el supuesto excepcional analizado.

Es por tanto deseable que, al menos mediante resoluciones judiciales, se avance en la aportación de elementos para un escrutinio más cercano a la seguridad jurídica propia de un estado de derecho.

Bibliografía

Bachmaier Winter, L. (2017). Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015. *Boletín del Ministerio de Justicia*, 2195, 1-38. Disponible en: https://bit.ly/1ksXy3m.

Díez-Picazo Giménez, L. M. (2008). *Sistema de derechos fundamentales*. Cizur Menor: Aranzadi.

Marchena Gómez, M. (2013). Proceso penal: nuevos problemas, viejas soluciones. *La Ley Penal*, 100, 1-13.

Martínez De Pisón Cavero, J. M. (2016). El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional. *Anuario de Filosofía del Derecho*, 32, 409-430.

Rebollo Delgado, L. (2005). *El derecho fundamental a la intimidad*. Madrid: Dykinson.

Rubio Alamillo, J. (2015). La informática en la reforma de la Ley de Enjuiciamiento Criminal. *Diario La Ley*, 8662, 1-11.

Ruiz Legazpi, A. (2014). Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (*incoming* de *Emule*) en la STC 173/2011. *Revista Española de Derecho Constitucional*, 100, 365-390.

Subijana Zunzunegui, I. J. (1997). Policía judicial y derecho a la intimidad en el seno de la investigación criminal. *Eguzkilore*, 10, 121-160. Disponible en: https://bit.ly/2JJ2wWW.

Zoco Zabala, C. (2015). *Nuevas tecnologías y control de las comunicaciones*. Cizur Menor: Aranzadi.