La investigación penal ante las nuevas tecnologías: reflexiones acerca de la «carga desproporcionada» y la «facilitación de información» en el registro de dispositivos de almacenamiento masivo de datos

BEATRIZ ESCUDERO GARCÍA-CALDERÓN
Profesora Contratada Doctora
CUNEF Universidad

RESUMEN

El presente trabajo pretende reflexionar acerca del concepto «carga desproporcionada» y de la expresión «facilitar información», introducidos en la Ley de Enjuiciamiento Criminal con la reforma operada por LO 13/2015, de 5 de octubre, y mantenidos en el Anteproyecto de Ley de Enjuiciamiento Criminal de 2020, para acotar el deber de colaboración en el contexto del registro de dispositivos de almacenamiento masivo de información.

Palabras clave: *carga desproporcionada; facilitación de información; deber de colaboración; registro de dispositivos de almacenamiento masivo de información; registro remoto.*

ABSTRACT

This paper intends to analyse the concept of «disproportionate burden» and the reference to the «provision of information», included both in the Spanish Criminal Procedure Act, as amended by Organic Law 13/2015 of 5 October, and in the 2020 Draft Criminal Procedure Act as limits to the duty of collaboration in the context of massive information storage devices searching.

Keywords: *disproportionate burden; provision of information; collaboration duty; mass information storage devices searching; remote searching.*

SUMARIO: 1. Planteamiento del problema: La investigación criminal después de sistema operativo iOS 8.–2. Consideraciones generales acerca del acceso a los dispositivos electrónicos en la LECRIM.–3. La regulación de los deberes de colaboración en las medidas de investigación tecnológica. A) La intervención de las comunicaciones telefónicas o telemáticas. B) El registro de dispositivos de almacenamiento masivo de información. C) El registro remoto de equipos informáticos. D) Las medidas de aseguramiento.–4. La regulación de los deberes de colaboración en el anteproyecto de LECRIM: El mantenimiento de la referencia a la carga desproporcionada.–5. Reflexiones acerca de la carga desproporcionada. A) Consideraciones generales. B) Ámbito de aplicación de la excepción. C) Criterios para determinar la desproporción de la carga. D) La creación de una puerta trasera como forma de colaboración exigible.–6. Observaciones acerca de la expresión «facilitar información». A) Interpretaciones posibles acerca del deber de facilitación de información. B) Propuesta de interpretación.–7. Conclusiones.–8. Bibliografía citada.

1. PLANTEAMIENTO DEL PROBLEMA: LA INVESTIGACIÓN CRIMINAL DESPUÉS DE SISTEMA OPERATIVO IOS 8

La proliferación del uso de dispositivos electrónicos ha provocado un correlativo incremento del interés de la Justicia en acceder a los datos que en ellos se contienen. No solo ha aumentado en los últimos años de manera exponencial la comisión de los denominados «ciberdelitos»(1), sino que también en los delitos tradicionales, ajenos a las nuevas tecnologías, los llamados teléfonos inteligentes han pasado a erigirse en una fuente probatoria capital. No en vano, autores y víctimas de delitos que podemos calificar de analógicos portan en sus móviles potentes dispositivos de geolocalización y una serie de instrumentos –una cámara de fotos, una grabadora de audio y vídeo y un modo de comunicarse con el exterior– que pueden ser utilizados durante la comisión del delito que protagonizan o padecen. Este tipo de evidencias(2) contenidas en los dispositivos electrónicos han sido bautizadas con el nombre de «prueba digital».

(1) Un revelador análisis estadístico sobre la cibercriminalidad en España en: http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3 (última consulta 12/2/2022).

(2) A este respecto, véase, por ejemplo, Blanco, H.: «El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre», *InDret* 1. 2021, p. 433; Sain, G. y Azzolin, H.: *Delitos informáticos,*

Lógicamente, el éxito en la búsqueda de pruebas digitales choca frontalmente con el uso, también en incesante crecimiento, de herramientas de control de acceso y cifrado, cuya utilización, más allá de estar permitida, es considerada esencial para garantizar la protección de determinados derechos fundamentales como son el derecho al secreto de las comunicaciones, el derecho a la intimidad y la libertad de expresión(3).

Por todo ello puede afirmarse que desde el nacimiento de las nuevas tecnologías existe una pugna lógica entre los encargados de la investigación criminal, interesados en acceder al contenido de los dispositivos, y las empresas digitales que, con el objetivo de lucrarse y bajo el pretexto de proporcionar seguridad y tranquilidad a sus usuarios, tratan de dificultar todo acceso no consentido a sus productos. Ello ha derivado en una suerte de competición, ciertamente desigual, entre un sector privado, que presta cobijo al delincuente con continuas mejoras técnicas garantes de su anonimato, y un sector público siempre a la zaga, pese a la excelente formación de sus técnicos y a los ingentes desembolsos económicos en los más avanzados dispositivos de desbloqueo y extracción de datos.

En cualquier caso, semejante pugna se ha mantenido hasta tiempos relativamente recientes dentro de lo que podríamos calificar como una desigualdad «aceptable», en la medida en que el Estado, con gran esfuerzo, acababa logrando el deseado acceso al dispositivo y con ello a las pruebas digitales que esclarecían lo ocurrido e incriminaban al delincuente.

En efecto, durante un largo periodo de tiempo, los investigadores han logrado introducirse en los dispositivos electrónicos protegidos mediante contraseñas recurriendo al mecanismo tradicional del denominado «ataque de fuerza bruta». De esta manera, y al igual que hicieran las primeras máquinas creadas durante la Segunda Guerra Mundial por los Aliados para descifrar los mensajes que los alemanes encriptaban gracias a la famosa máquina «Enigma», el investigador criminal introducía todas las combinaciones numéricas posibles hasta dar con la adecuada.

---

*Investigación criminal, marco legal y pe*ritaje, IBdef, Montevideo-Buenos Aires, 2017, pp. 12-14; Poveda Criado, M. A.: *Delitos en la Red*, Fragua, Madrid, 2015, pp. 156, que distingue entre evidencia electrónica y evidencia digital, pp. 153-157.

(3) Una enumeración de los distintos derechos afectados según la medida de investigación en Richard González, M.: «La investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal*, núm. 43, septiembre 2017, p. 17.

Ante el éxito del investigador público, que antes o después lograba su propósito de acceder al contenido del dispositivo, las empresas tecnológicas dieron un paso más y convirtieron las contraseñas en algoritmos de gran complejidad. Un hito, en este sentido, lo constituyó la creación del AES-256, que representa el estándar de encriptación más avanzado que se conoce a día de hoy. No obstante, como seguía tratándose entonces de un problema de cálculo matemático y de tiempo, lo único que requería el investigador para garantizarse el acceso al dispositivo cifrado era un aumento en la velocidad y la potencia de cálculo. La solución llegaría entonces de la mano de las «supercomputadoras» que, gracias al funcionamiento simultáneo de sus cientos de procesadores por medio del bautizado como «trabajo en paralelo», permitirían lograr el deseado acceso a la prueba digital todavía unos años más.

El panorama cambiaría, sin embargo, de manera radical a partir de 2014. Ese año *Apple* saca al mercado un sistema operativo, el iOS 8, cuyas mejoras técnicas dejarían al sector público fuera de esa competición. En efecto, esta nueva versión introduciría, por un lado, un sistema de retardo que provocaba una paulatina ralentización en el propio sistema tras la inserción de una contraseña fallida, no admitiendo una nueva contraseña hasta que hubiera transcurrido un tiempo determinado. Ese tiempo aumentaba exponencialmente tras cada intento, de manera que, después de unas cuantas contraseñas erróneas, había que esperar años para poder introducir la siguiente. Con esta medida se acababa con la posibilidad de recurrir a la fuerza bruta para acceder a un dispositivo electrónico, lo que equivalía a dejar a la investigación criminal herida de muerte. Y por si esto fuera poco, el iOS 8 introdujo una segunda medida letal para la investigación criminal: un sistema de autodestrucción de datos que el usuario podía habilitar y que provocaba que, tras diez de esos intentos fallidos, la información contenida en el dispositivo fuera borrada automáticamente.

Con semejantes innovaciones técnicas, el sector público quedaba fuera de la carrera, al menos en lo relativo a los productos con el logo de la manzana. La innovación introducida por *Apple* generó, además, un lógico efecto imitación por parte de sus competidores, de manera que todas las empresas tecnológicas pasaron a instalar de serie en los dispositivos que sacaban al mercado complejos sistemas de acceso y de cifrado de datos. La protección de la confidencialidad del usuario –y la consiguiente debilidad del Estado– se generalizó. También los servicios de comunicación, desde *WhatsApp* hasta *Zoom*, pasaron al llamado «cifrado de extremo a extremo»(4), e incluso en Internet

(4) Se denomina «de extremo a extremo» porque el mensaje es cifrado en el extremo del remitente, viaja cifrado, y llega cifrado al extremo del destinatario, que es

empezaron a ofrecerse de manera gratuita sistemas de encriptación de datos, como el *GnuPG*, *7-ZIP*, *AES Crypt*, *Diskryptor*, *BitLocker*, *MEO* y *VeraCrypt*, entre otros.

En este nuevo escenario el investigador público perdió toda libertad y autonomía y en lo relativo al acceso a los dispositivos electrónicos pasó a depender irremediablemente de la ayuda del sector privado. El legislador, consciente de esa relación de dependencia y de los intereses muchas veces contrapuestos de ambos sectores, incluyó en la reforma de la Ley de Enjuiciamiento Criminal (en adelante, LECrim) operada por LO 13/2015, de 5 de octubre(5), una serie de deberes de colaboración sobre el sector privado que garantizaran al sector público el acceso a la prueba digital. Esos deberes, y sus límites, se han mantenido con ciertos retoques en el texto del Anteproyecto de Ley de Enjuiciamiento Criminal de 2020. Al análisis de unos y otros dedicaremos las líneas que siguen.

2. CONSIDERACIONES GENERALES ACERCA DEL ACCESO A LOS DISPOSITIVOS ELECTRÓNICOS EN LA LECRIM

Como es sabido, con la importante reforma operada en la LECrim por la LO 13/2015, de 5 de octubre, se reguló por primera vez en España el registro de dispositivos electrónicos, cuestión que hasta entonces se encontraba en una situación de alarmante vacío normativo. Las disposiciones contenidas en el Convenio de Budapest de 2001 sobre ciberdelincuencia, ratificado por España en el año 2010, resultaban insuficientes y excesivamente genéricas. Las numerosas lagunas existentes eran suplidas por la jurisprudencia a través de una constante adaptación de las instituciones tradicionales y de un recurso incesante a la analogía.

Prueba de la precariedad de la situación lo constituía el hecho de que, hasta la reforma de la LECrim, el acceso a los datos contenidos en los dispositivos electrónicos se regía por los preceptos tradicionales relativos al registro de libros y papeles y recogida de otros efectos e instrumentos del delito. Los jueces de instrucción y de la policía, ante la obsolescencia de las normas procesales, incompatibles con las exi-

---

el único que puede descifrarlo. Por oposición a este sistema, en el llamado «cifrado de datos en tránsito», los mensajes se cifran en el extremo del remitente, pero al llegar al servidor son descifrados y cifrados nuevamente, para descifrarse finalmente al llegar al destinatario.

(5) Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el reforzamiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (*BOE* núm. 239, de 6.10.2015).

gencias que planteaba el nuevo mundo digitalizado, debían –parafraseando al juez Marchena(6)– recurrir a la imaginación en demasiadas ocasiones(7). Urgía, pues, la elaboración de una normativa específica que adaptara el Derecho procesal penal al nuevo escenario donde había pasado a desarrollarse la actividad criminal tras la revolución tecnológica. Sin embargo, hizo falta todavía una sentencia del Tribunal Constitucional(8) que, al declarar la nulidad de una medida probatoria –en concreto, de unas grabaciones obtenidas mediante la colocación de micrófonos en la celda de una comisaría, por vulnerar el derecho al secreto de las comunicaciones– precipitaría la ansiada reforma.

No obstante, el acometimiento de semejante tarea legislativa no era, sin embargo, sencillo, pues a las dificultades lógicas derivadas de la exigencia de conocimientos técnicos específicos(9) se sumaba la dificultad añadida de que un mismo acceso podía vulnerar derechos diferentes y con distinta protección constitucional. Así, y a título meramente ejemplificativo, los correos electrónicos, los mensajes, las fotos, los datos bancarios y los datos relativos a la geolocalización que coexisten en un mismo dispositivo, se corresponden con bienes jurídicos

(6) Manuel Marchena es un acreditado experto en nuevas tecnologías. Sin ninguna pretensión de exhaustividad, destacan entre sus publicaciones, por ejemplo: «Algunos aspectos procesales de Internet», en *Problemática jurídica en torno al fenómeno Internet*, Cuadernos de Derecho Judicial, Escuela Judicial, Consejo General del Poder Judicial, 2000; «El sabotaje informático: entre los delitos de daños y desórdenes públicos», *Actualidad informática Aranzadi: revista de informática para juristas*, núm. 40, 2001 y «Dimensión jurídico-penal del correo electrónico», publicado en *Estudios jurídicos*, núm. 2007. En 2012 fue designado Presidente de la Comisión Institucional creada para la elaboración de una propuesta de reforma de la Ley de Enjuiciamiento Criminal. Es autor, junto al catedrático de Derecho procesal Nicolás González-Cuéllar de la obra de referencia *La Reforma de la Ley de Enjuiciamiento Criminal de 2015*, Ediciones Jurídicas Castillo de Luna, Madrid, 2015. De alguna de sus intervenciones públicas se informa, por ejemplo, en https://www.20minutos.es/noticia/4149329/0/el-juez-marchena-sobre-el-uso-de-las-nuevas-tecnologias-todos-vamos-dejando-un-rastro-que-nos-hace-transparentes/ y en https://www.diariodenavarra.es/noticias/navarra/2020/02/12/el-juez-marchena-alerta-universidad-navarra-vinculacion-entre-nuevas-tecnologias-delito-680623-300.html (último acceso a ambos links 1/2/2022).

(7) En este sentido, en el Preámbulo de la LO 13/2015, de 5 de octubre, se afirma que «por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado».

(8) STC 145/2014, de 22 de septiembre.

(9) Acerca de las numerosas complejidades técnicas y de todo tipo que la materia plantea puede verse Rubio Alamillo, J.: «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *Diario La Ley*, núm. 8662, 2015, pp. 1-12.

diversos, de manera que con el acceso al dispositivo, dependiendo de la información que se encuentre, unas veces puede verse afectado, por ejemplo, al derecho a la intimidad o derecho a la protección de datos, y otras, al derecho al secreto de las comunicaciones, que como es sabido, goza de un nivel de protección constitucional superior. No en vano, con el objeto de proporcionar un tratamiento unitario se propone incluso englobar todos estos derechos en un único espacio de exclusión que se ha dado en denominar «derecho al entorno virtual»(10).

Sorteados o no todos los obstáculos, podemos afirmar que con la reforma de la LECrim por medio de la LO 13/2015, de 5 de octubre, el legislador ha optado, en líneas generales, por una regulación singularmente garantista a la hora de obtener la prueba digital. Introduce como nuevas medidas de investigación el registro de dispositivos de almacenamiento masivo y el registro remoto de equipos informáticos. A su vez, dentro del registro de dispositivos de almacenamiento masivo diferencia el acceso a dispositivos aprehendidos con ocasión de un registro domiciliario, los incautados fuera del mismo, y el registro ampliado a través del que está siendo objeto de registro físico (el llamado *cloud computing*). Para todo tipo de acceso se exige la resolución judicial habilitante, no bastando ya, al contrario de como se venía haciendo antes de la entrada en vigor de la reforma de 2015, la cobertura que proporciona la autorización judicial para el registro domiciliario. Dicha resolución, salvo el caso del registro remoto(11), podrá ser posterior y tener un carácter convalidante siempre y cuando la

(10) A favor de este tratamiento unitario, por todas, ya la STS 823/2015, de 28 de febrero. Respecto a los diferentes derechos afectados, puede verse Zaragoza Tejada, J. I.: «El registro de dispositivos de almacenamiento masivo de la información», en la obra dirigida por él, *Investigación tecnológica y derechos fundamentales*, Thomson Reuters Aranzadi, Pamplona, 2017, pp. 408-420. En la importante STS 489/2018, de 23 de octubre, se afirma (FJ 5): «Algunos precedentes alientan la aparición de un derecho vinculado a los mencionados, pero con cierta vocación de emanciparse para cobrar autonomía e identidad propias. Partiendo de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (*smartphone*) se conviene en la necesidad de un tratamiento unitario a partir de la proclamación de un derecho al entorno digital. Sería un derecho de nueva generación que serviría para alumbrar y justificar distintos escalones de protección jurisdiccional (SSTS 342/2013, de 17 de abril; 587/2014, de 24 de febrero, y 587/2014, de 18 de julio)». En el mismo sentido se pronuncia más recientemente la STS 462/2019, de 14 de octubre (FJ 1).

(11) Aunque ello ha sido objeto de duras críticas. En contra de no permitir el registro remoto sin autorización judicial en casos de urgencia, por ejemplo, Montes Álvaro, M. A.: «La regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el artículo 18 CE», *Revista del Ministerio Fiscal*, año 2017, núm. 3, p. 116.

urgencia impida obtener la autorización judicial con anterioridad al acceso. Lógicamente, puesto que todas estas injerencias afectan a derechos fundamentales, solamente estarán legitimadas en la medida en que se lleven a cabo respetando los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, como reglas que orientan y rigen la investigación tecnológica en su conjunto(12).

3. LA REGULACIÓN DE LOS DEBERES DE COLABORACIÓN EN LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

A grandes rasgos, y de acuerdo con la propia clasificación que establece la Ley, cuatro son los grupos o momentos principales en los que pueden agruparse estas obligaciones de cooperar en la investigación tecnológica(13): la relativa a la intervención de las comunicaciones telefónicas o telemáticas, la que tiene que ver con el registro de dispositivos de almacenamiento masivo de información, la que hace referencia a los registros remotos de equipos informáticos y, por último, la que se exige para garantizar la conservación de datos.

A la delimitación del contorno de esas obligaciones de cooperar, junto con otras importantes cuestiones, se han dedicado diversas Circulares de la Fiscalía General del Estado (en adelante, FGE) del año 2019(14). Veamos brevemente en qué consisten estos deberes, no

(12) Véase Marchena Gómez, M. y González-Cuéllar Serrano, N.: *La Reforma de la Ley de Enjuiciamiento Criminal de 2015*, *op. cit*., pp. 211-216.

(13) Más adecuado hubiera sido probablemente, como indicaba ya el Consejo de Estado en su Informe y recuerda Sánchez Melgar, haber introducido un deber de colaboración unitario y suficientemente amplio en las disposiciones comunes que actúan como principios rectores –esto es, en 588 bis a a k, y en los capítulos sucesivos. Puede leerse la opinión de Sánchez Melgar, J., en la Encuesta Jurídica publicada por Sepín en octubre de 2016, disponible en https://sepin.es/cronus4plus/documento/VerDoc.asp?dist=55&referencia=SP%2FDOCT%2F21122&cod=0JP2JP1Cv0FF1T10Vb0FP1%24v0GC0Fa1yB0G909P17P0Vf08A1ek1S308A1vd1yi05u1dF1Dk0Ha1%3DP01b0Fa17T1DT0Fk1C50Gz0Fa1Aa01f0Ha1Aa1Dg0Fa1C42AA0G%5F1C51Cv0FF0yg0HL0GB0Oq01E#25605745 (último acceso 6/3/2022).

(14) En concreto, estas cinco: Circular 1/2019, de 6 de marzo de 2019, de la Fiscalía General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal; Circular 2/2019, de 6 de marzo de 2019, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas; Circular 3/2019, de 6 de marzo de 2019, de la Fiscalía General del Estado, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; Circular 4/2019, de 6 de marzo de 2019, de la Fiscalía General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización;

sin antes recordar que la prueba digital plantea numerosos problemas procesales, entre los que destacan los de carácter jurisdiccional –como el de la determinación de la localización de los datos que constituyen la evidencia digital(15), especialmente cuando se trata del registro remoto de datos que se encuentran en servidores o en la nube–, y el de la admisibilidad de la prueba transnacional(16). Ello ha llevado incluso a algún autor a proponer una reformulación de los conceptos de territorialidad y jurisdicción.

Precisamente, la principal barrera a la hora de hacer efectivo un deber de colaboración vendrá impuesta por el hecho de que la empresa extranjera no se sentirá vinculada por la orden de un juez español(17). Por todo ello, la verdadera efectividad de la investigación criminal en los delitos vinculados con sistemas informáticos dependerá de la eficacia de los instrumentos de cooperación judicial penal existentes en el ámbito internacional(18), habida cuenta de que en la gran mayoría de los casos el obligado a colaborar se encontrará fuera de nuestro territorio. Sin una cooperación penal eficaz, los mandatos contenidos en la LECrim quedan reducidos a una mera declaración de intenciones.

De ello fue consciente también el Convenio de Budapest ya en el año 2001, al establecer las bases para la cooperación entre Estados en

---

y Circular 5/2019, de 6 de marzo de 2019, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos.

(15) Por todos, Ortiz Pradillo, J. C.: «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica», en Pérez Gil, J. (coord.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, La Ley, Madrid, 2012, p. 278.

(16) Ya advertía de estos problemas Bachmaier Winter, L.: «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *Boletín del Ministerio de Justicia*, año LXXI, núm. 2195, enero 2017, pp. 26 y 27.

(17) De ahí que Bermúdez González afirme: «Otra cosa será que dicha intervención sea técnicamente factible. O que las compañías extranjeras que facilitan estos servicios se sientan vinculadas por la legislación española». Con argumentos similares augura Rodríguez Lainz a este deber «dudosas probabilidades de éxito». Véanse, respectivamente, Bermúdez González, J. A.: «Deber de colaboración de particulares en la Ley de Enjuiciamiento Criminal», Ponencia presentada en el Curso de formación de Fiscales «Uso de las nuevas tecnologías y nuevas formas de delincuencia», celebrada en el Centro de Estudios Jurídicos los días 27 y 28 de octubre de 2016, p. 7, disponible en www.cej-mjusticia.es (último acceso 27/2/2022) y Rodríguez Lainz, J. L: «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?», *Diario La Ley*, núm. 8729, 2016, pp. 11-13.

(18) Acerca de los problemas relativos a la jurisdicción que plantea la persecución de los ciberdelitos puede verse Velasco San Martín, C.: *Jurisdicción y competencia en relación al acceso transfronterizo en materia de ciberdelitos, op. cit*., pp. 169-224.

esta materia(19), y ello será tenido en cuenta con seguridad en el nuevo Ciberconvenio que vendrá a reemplazarlo y cuya elaboración ya está en marcha. Recordemos, a este respecto, que el 26 de mayo de 2021 la Asamblea General de la ONU adoptó la resolución 75/282 relativa a la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos, y que el 29 de marzo de 2022 se ha publicado una «Recomendación de Decisión del Consejo por la que se autorizan las negociaciones de un convenio internacional integral sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos» (20). Se avecinan, pues, cambios normativos, que aconsejan tener en cuenta los déficits en la regulación actual para su corrección.

A) **La intervención de las comunicaciones telefónicas o telemáticas**

Hasta la reforma de la LECrim operada en 2015(21), la regulación dedicada a los deberes de colaboración resultaba tremendamente insatisfactoria. Por un lado, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, limitaba el deber de conservación de datos «a los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones»; por otro, la Ley General de Telecomunicaciones restringía también la imposición del deber de interceptar las comunicaciones a «los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público» (art. 39.1 LGT)(22).

Además, mientras que las operadoras de telecomunicaciones resultaban obligadas a conservar y a ceder datos a los denominados «agen-

(19) Sobre esa cooperación puede verse, por ejemplo, Ortiz Pradillo, J. C.: *Problemas procesales de la ciberdelincuencia*, Colex, Madrid, 2013, pp. 76-80.

(20) Texto disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52022PC0132&from=EN (último acceso 20/3/2022).

(21) De entre las diversas modificaciones que ha sufrido la LECrim en 2015, nos referiremos exclusivamente a la realizada por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

(22) Los operadores están obligados, según reza el apartado segundo del artículo 39, a «realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica».

tes facultados»(23), quedaban eximidos de este deber los prestadores de servicios. Consideramos a estos efectos especialmente ilustrativas las palabras de Bermúdez González acerca de quiénes quedaban obligados a colaborar: «por poner nombres y apellidos: Movistar, Vodafone y Orange, sí; Google, Microsoft, Facebook o Amazon, no»(24).

Con el objetivo de corregir estas insuficiencias, la reforma de la LECrim de 2015 introdujo un deber de colaboración relativo a la intervención de las comunicaciones telefónicas o telemáticas que afectaría, de acuerdo con el artículo 588 ter e. 1 LECrim, a «todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual (…)». Tras la reforma, son destinatarios de ese deber de colaboración, tal y como especifica la Circular 2/2019, «desde las más importantes compañías de telecomunicaciones hasta el simple particular que intermedie en el proceso de comunicación»(25). Con ello se ha pretendido poner fin a la falta de colaboración existente hasta entonces, ya que por más que señale la misma Circular 2/2019 que «el precepto no hace más que enfatizar expresamente para los supuestos de interceptación de comunicaciones la obligación de colaboración con Jueces y Tribunales que, con carácter general, recogen los artículos 118 CE y 17.1 LOPJ», lo

(23) Se trata de los miembros de los Cuerpos Policiales, personal del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial.

(24) Bermúdez González, J. A.: «Deber de colaboración de particulares en la Ley de Enjuiciamiento Criminal», *op. cit*., p. 7. También indica Bermúdez González que, con la nueva regulación, «tan obligada queda una compañía de telecomunicaciones tradicional, que suministre acceso a la red telefónica, como una compañía de videojuegos online».

(25) Véase el apartado 7, «Deber de colaboración», disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4241 (último acceso 20/2/2022). Actualmente tres son, pues, los sujetos vinculados con este deber de colaboración: los prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones, los prestadores de servicios de la sociedad de la información, y cualquier otra persona que de algún modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. En definitiva, está obligado a colaborar todo sujeto que sepa cómo se accede al contenido del dispositivo, bien porque conoce el funcionamiento del sistema informático o bien porque conoce las medidas aplicadas para proteger los datos. Lo que ha de entenderse comprendido en cada grupo de sujetos es explicado y especificado en la Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

cierto es que no todos los encargados de las comunicaciones se sentían vinculados por semejante deber general.

La regulación en la LECrim cierra con una breve referencia al deber de sigilo de los obligados a colaborar y a la posibilidad de castigar por un delito de desobediencia tanto la negativa a colaborar como el incumplimiento de ese deber de sigilo.

En todo caso, resulta reseñable que en la redacción inicial del Anteproyecto se excluyera de semejante obligación «al sospechoso o imputado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional», referencia que ha sido suprimida en el texto definitivo. No obstante, dicha supresión no es debida a que la voluntad del legislador fuera la de que no rigiera dicha excepción para este supuesto. Su razón de ser reside más bien en que, tras haber aconsejado el Consejo Fiscal alternativamente en distintos lugares del informe, bien un cambio de ubicación de la excepción o bien la inclusión de una cláusula de remisión(26), se optó por su inclusión únicamente en el artículo 588 sexies c, precepto dedicado al registro de dispositivos de almacenamiento masivo de información.

B) **El registro de dispositivos de almacenamiento masivo de información**

De acuerdo con el artículo 588 sexies c, párrafo 5, «las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia». Por lo tanto, con respecto a los dispositivos de almacenamiento masivo de datos(27), el párrafo 5 del artículo 588 sexies c LECrim permite a las

(26) Se plantea en el Informe que «quizás sea más operativo la inclusión en este punto de una cláusula de remisión». Véase el «Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», p. 121.

(27) A pesar de que la utilización de los términos «dispositivo» y «masivo» puede llevar a equívoco en la medida en que el término dispositivo parece exigir un soporte físico de carácter físico, y que el adjetivo «masivo» parece requerir una enorme capacidad. Sin embargo, no es cierto ni lo uno ni lo otro. Como indica Ber-

autoridades y agentes ordenar la facilitación de la información necesaria a cualquiera que conozca el funcionamiento del sistema informático o las medidas de seguridad que protegen los datos, bajo amenaza de incurrir en delito de desobediencia. Semejante obligación rige aun cuando el sujeto no tenga relación con el sistema objeto de registro. Tal sería el caso de los fabricantes de los dispositivos o de los terceros que dispongan de conocimientos sobre la seguridad del dispositivo o la localización de los datos, como los *hackers*.

No obstante, los destinatarios quedan eximidos del deber de cooperar cuando de la colaboración se derive para ellos una «carga desproporcionada». Se traspone así prácticamente el artículo 19.4 del Convenio de Budapest, que establece un deber de facilitar información limitado igualmente por una cláusula de proporcionalidad. También se detrae expresamente del círculo de obligados, en todo caso, al «investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional»(28).

C) **El registro remoto de equipos informáticos**

En el supuesto de los registros remotos, el deber de colaboración alcanza a un mayor número de sujetos que en el registro de dispositivos de almacenamiento masivo. Su contenido resulta también más amplio.

Así, por un lado, en el apartado 1 del artículo 588 septies b. LECrim contempla un deber de colaboración de amplísimo espectro que tiene como destinatarios a los prestadores de servicios y personas señaladas en el artículo 588 ter e.1 LECrim (es decir, a «Todos los prestadores de servicios de telecomunicaciones, de acceso a una red

---

múdez González, basta cualquier soporte de almacenamiento de datos con independencia de su capacidad y de su localización: un *pen drive* o un teléfono móvil de escasa capacidad se encuentran afectados por esta regulación y también lo está el acceso a la información recogida en servidores remotos de almacenamiento, conocidos popularmente como «la nube». Respalda su opinión en el argumento jurídico de que el artículo 588 sexies a habla de la «aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos». Véase Bermúdez González, J. A.: «Deber de colaboración de particulares en la Ley de Enjuiciamiento Criminal», Ponencia presentada en el Curso de formación de Fiscales «Uso de las nuevas tecnologías y nuevas formas de delincuencia», *op. cit.*, pp. 7 y 8.

(28) Esta cuestión la traté en «El investigado o encausado, el abogado y el pariente como sujetos excepcionados del deber de colaborar en la obtención de la prueba digital», *Revista General de Derecho Penal*, núm. 36, 2021, pp. 1-44.

de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual») y a los titulares o responsables del sistema informático o base de datos. Todos estos sujetos quedan obligados «a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización», de manera que, en caso de negarse a cooperar, incurrirían en un delito de desobediencia.

Este tipo de investigación resulta muy agresiva, pues normalmente se realiza por medio de los denominados *spywares,* que son *softwares* instalados a distancia con los que se consigue el *hackeo* de un sistema informático, aprovechando la vulnerabilidad del sistema al que se accede a través de las llamadas *exploits*. Su instalación, por tanto, aunque requiere de la –involuntaria– colaboración del titular del dispositivo, se lleva a cabo sin su conocimiento. Con los *spywares* pueden llevarse a cabo todo tipo de actividades destinadas a obtener pruebas digitales, desde extraer los datos contenidos en el dispositivo, hasta realizar escuchas y grabaciones. Es posible, incluso, conocer los datos cifrados mediante las denominadas «encriptaciones fuertes» o las contraseñas del usuario a través de los llamados *keyloggers*(29), que registran las teclas pulsadas. A la creación e inoculación de un *software* de este tipo quedarían obligados los sujetos afectados por el deber de colaboración.

El apartado 2, por su parte, reproduce el deber de colaboración previsto para el registro de dispositivos de almacenamiento masivo del artículo 588 sexies c.5 LECrim, al permitir que las autoridades y los agentes encargados de la investigación ordenen «a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria» bajo amenaza de incurrir en delito de desobediencia. También se exime de esta obligación, al igual que en el caso del registro de dispositivos de almacenamiento masivo, al investigado o encausado, a su abogado y a los

(29) Con arreglo a la definición prevista en GIL GIL, A. y HERNÁNDEZ BERLINCHES, R. (coords.): *Cibercriminalidad*, Dykinson, Madrid, 2019, p. 65, «los *Keyloggers* son un tipo de *malware* que es capaz de monitorizar las pulsaciones de teclas en el teclado memorizándolas en un fichero para posteriormente remitirlas a un tercero. Existen variantes que realizan capturas de pantallas o movimientos y pulsaciones de ratón. Se utiliza para la obtención de las credenciales de autenticación, datos bancarios o monitorización de conversaciones, entre otros usos».

dispensados de declarar por razón del parentesco. Por último, es preciso subrayar que no se contiene en el artículo 588 septies b LECrim, dedicado al deber de colaboración en el registro remoto, referencia alguna al principio de proporcionalidad.

D) **Las medidas de aseguramiento**

En el capítulo X, dedicado a las medidas de aseguramiento, la reforma operada por LO 13/2015, de 5 de octubre, añadió un artículo único, el 588 octies, que regula la orden de conservación de datos y permite que el Ministerio Fiscal o la Policía Judicial requieran «a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión (…)». Esa obligación de conservación existe «durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.» Sobre el requerido a colaborar pesa un deber de guardar secreto, «quedando sujeto a la responsabilidad descrita en el apartado·3 del artículo 588 ter e». En definitiva, se prevé la posibilidad de que el sujeto incurra en la comisión de un delito de desobediencia.

4. LA REGULACIÓN DE LOS DEBERES DE COLABORACIÓN EN EL ANTEPROYECTO DE LECRIM: EL MANTENIMIENTO DE LA REFERENCIA A LA CARGA DESPROPORCIONADA

En el Anteproyecto de Ley de Enjuiciamiento Criminal de 2020 no solamente varía la numeración de los artículos, sino que el contenido de alguno de ellos también sufre notables modificaciones. La ahora denominada «intercepción» de las comunicaciones telefónicas o telemáticas pasa al Capítulo II, y los destinatarios del deber de colaboración del artículo 588 ter e se mantienen, de manera explícita esta vez y no por remisión, en el artículo 361 del Anteproyecto: «todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual». En la

nueva normativa, sin embargo, se suprime la referencia «al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida» como acreedores de esa colaboración, consistente en «la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones» y se establece, de manera más simple, que aquellos sujetos «están obligados» –sin decir con quién– «a prestar la colaboración que les sea requerida para la práctica de la diligencia de intervención, grabación o registro».

Por lo que respecta al registro de dispositivos de almacenamiento masivo de información y al registro remoto sobre equipos informáticos, estos pasan a regularse, respectivamente, en los Capítulos III y IV del Título IV, dedicado a los medios de investigación relativos a la entrada y registro, intervención de libros, papeles y documentos y registros informáticos.

Así, en el artículo 428 del Anteproyecto se recogen ahora los deberes de colaboración del registro directo, con una redacción muy similar a la del primer párrafo del apartado 5 del artículo 588 sexies c. LECrim: «Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos en él contenidos que facilite la información que resulte necesaria para acceder a dichos datos, siempre que de ello no derive una carga desproporcionada para la persona afectada, bajo apercibimiento de incurrir en delito de desobediencia». Continúa, pues, la mención a la desproporción de la carga como límite objetivo al deber de colaboración, pero se introduce una precisión que aclara el alcance del deber: la información que se ha de facilitar es la «que resulte necesaria para acceder a dichos datos». También se reforma el párrafo segundo, donde se contienen los sujetos exceptuados del deber de colaborar, con una redacción mucho más acertada, de manera que ya no se deja fuera de la excepción a quien necesariamente ha de estar comprendido en ella por exigencias del secreto profesional(30).

Por su parte, el artículo 432 de la nueva LECrim se ocupa del «deber de colaboración» –en singular–, del registro a distancia. Los destinatarios son los mismos que en el artículo 588 septies b, si bien no se utiliza ninguna remisión (como la que sí hace el 588 septies b al 588 ter), mencionándose todos expresamente. Se mantiene en el apartado 3 el deber de sigilo de los sujetos requeridos, pero la nueva redacción elimina el apartado 4, que hace referencia a la responsabili-

(30) *Ibidem*, p. 26.

dad por delito de desobediencia. En las medidas de aseguramiento (art. 588 octies LECrim; art. 433 en el Anteproyecto) también se suprime la amenaza de incurrir en un delito de desobediencia y simplemente se recuerda en el artículo 435 la obligación de prestar colaboración y guardar secreto, pero sin hacer mención de la correspondiente sanción en caso de incumplimiento.

Por lo tanto, y a modo de recapitulación: aunque son varias y de calado las modificaciones que introduce el Anteproyecto de Ley de Enjuiciamiento Criminal de 2020 en lo relativo a los deberes de colaboración, en lo que respecta a la «carga desproporcionada», que es lo que aquí interesa, la regulación se mantiene idéntica, con la misma redacción y contenida también en el registro directo de dispositivos de almacenamiento masivo. De esta manera, lo que se va a decir a continuación tiene validez tanto para la regulación vigente como para el nuevo texto legal, cuando entre en vigor.

5. REFLEXIONES ACERCA DE LA CARGA DESPROPORCIONADA

A) **Consideraciones generales**

Como venimos señalando, el legislador ha introducido dos límites al deber de colaboración que se mantienen en el Anteproyecto de Ley de Enjuiciamiento Criminal: un límite objetivo, constituido por la aplicación del principio de proporcionalidad, y un límite de carácter subjetivo, que excluye de este deber de colaborar a determinados sujetos.

El primer límite al deber de colaboración viene dado por la aplicación del principio de proporcionalidad: de acuerdo con el artículo 588 sexies c.5 de la actual LECrim y con el artículo 428 del Anteproyecto, de las órdenes que han de acatarse en cumplimiento del deber de colaboración quedan descartadas aquellas de las que pueda derivarse una «carga desproporcionada» para el afectado. Por carga desproporcionada deberá entenderse toda obligación que conlleve un gravamen excesivo para el afectado(31).

En este sentido, el artículo 588 bis a 5 establece que las medidas de investigación se considerarán proporcionadas solamente cuando

(31) Sobre los debatidos conceptos de proporcionalidad en sentido amplio y estricto, véase, por ejemplo, Navarro Frías, I.: «El principio de proporcionalidad en sentido estricto: principio de proporcionalidad entre el delito y la pena o balance global de costes y beneficios», *Indret* 2/2010, pp. 13 ss.

«tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros». Y añade que «para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia perseguida con la restricción del derecho». En definitiva, como indica González-Cuéllar Serrano, el principio de proporcionalidad «requiere que toda limitación de derechos tienda a la consecución de fines legítimos»(32).

Surgen así dos cuestiones de sumo interés que serán objeto de examen. En primer lugar, se analizará si el hecho de que el legislador haya omitido la referencia a la desproporción de la carga en la interceptación de comunicaciones, en el registro a distancia y en las medidas de conservación significa que solamente puede oponerse esa excepción en el registro directo.

En segundo lugar, reflexionaremos acerca de las condiciones que han de darse para poder afirmar la desproporción de la carga, y al hilo de esta cuestión, analizaremos la posible oposición de una excepción como ésta en aquellos casos en los que se requiere de la colaboración de una empresa tecnológica.

Como es sabido, en diversas ocasiones en que se ha solicitado a *Apple* su colaboración en la investigación de un delito, la empresa de la manzana ha accedido a proporcionar la información que se encuentra en los servidores remotos de almacenamiento conocidos como «la nube», y sin embargo se ha negado siempre a la creación de una puerta trasera (*backdoor*). Las denominadas puertas traseras constituyen un medio para acceder a un sistema informático o al contenido de unos datos cifrados eludiendo los mecanismos de seguridad. Esos accesos pueden crearse involuntariamente, fruto de un error de programación, o voluntariamente, como medio empleado por los programadores para acceder al sistema y llevar a cabo labores de mantenimiento o actualización del dispositivo. Es posible también crear un acceso de este tipo *a posteriori*, por ejemplo, a través de un *malware*(33). Como es conocido por todos, la empresa *Apple* ha negado su colaboración en EE UU en diversas ocasiones(34) cuando así lo ha solicitado el FBI, adu-

(32) González-Cuéllar Serrano, N.: «El principio de proporcionalidad en el Derecho penal español», *Cuadernos de Derecho público*, núm. 5, 1998, p. 193.

(33) A este último tipo de puerta trasera se hace referencia en Gil Gil, A. y Hernández Berlinches, R. (coords.): *Cibercriminalidad*, *op. cit*., p. 64.

(34) El caso más conocido es el del tiroteo de San Bernardino. Véase: https://elpais.com/internacional/2016/02/17/actualidad/1455702891_642434.html (último

ciendo principalmente los peligros que supone la creación de una puerta trasera y a los daños reputacionales que ello supondría para la marca, y ha considerado suficiente su colaboración al proporcionar los datos contenidos en la nube.

Haremos referencia, pues, a la posibilidad de que las empresas se acojan a la desproporción de la carga como argumento para rechazar la negativa a cooperar en la investigación tecnológica, si un conflicto como el sucedido en EE. UU. se diera en nuestro país, como lógicamente sucederá en un futuro no lejano con toda probabilidad(35).

B) **Ámbito de aplicación de la excepción**

Como cuestión inicial, cabe plantearse si el hecho de que la norma haga referencia a ese límite objetivo de la desproporción de la carga únicamente al regular el registro directo de dispositivos de almacenamiento masivo de la información ha de entenderse en el sentido de que solamente es en ese ámbito donde esta limitación resulta oponible. Es decir, si el legislador ha querido que esta excepción no rija en la intervención de las comunicaciones, ni en los registros remotos o en la orden de conservación de datos. Creemos que la respuesta a esta cuestión ha de ser necesariamente negativa: ni parece que el legislador quiera verdaderamente reducir la vigencia de tal restricción a este ámbito, ni tendría sentido tampoco que quisiera limitar justamente el registro donde la afectación del secreto de las comunicaciones, como pone de manifiesto Zaragoza Tejada(36), es menor.

---

acceso 6/3/2022) Pero no es el único. En España también tuvimos conocimiento de la necesidad de acceder al contenido del dispositivo, por ejemplo, en el caso Diana Quer. Véase: https://elpais.com/politica/2017/07/06/actualidad/1499325032_475830.html (último acceso 6/3/2022).

(35) Afirma Rodríguez Lainz, J. L.: «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?», *op. cit.,* p. 11, que «en la estrategia jurídica conocida empleada por APPLE no se ha llegado a cuestionar el carácter manifiestamente desproporcionado de tal cometido; sino más bien, el daño a su reputación comercial, la ausencia de una norma que específicamente habilitara a la autoridad judicial para imponer ese deber de colaboración y el riesgo de afectación a la seguridad de todos sus sistemas como consecuencia de la creación de lo que se definiera como una auténtica puerta trasera». En efecto, en EE. UU. no se ha hecho referencia a esa desproporción de manera expresa, entre otras cosas porque la ley estadounidense no recoge una cláusula como la española. Ahora bien, entendemos que el daño reputacional y el peligro que generaría una puerta trasera constituyen manifestaciones de una posible desproporción y que como tales podrían oponerse en nuestro país.

(36) Zaragoza Tejada, J. I.: «El registro remoto de equipos informáticos», *op. cit.,* pp. 445-447.

Consideramos que el límite de la carga desproporcionada resulta aplicable a todos los ámbitos en los que se imponen deberes de colaboración porque, en realidad, esa expresión no constituye más que una referencia expresa al principio de proporcionalidad característico de todas las medidas de investigación, tecnológicas o no, en las que se ven afectados derechos fundamentales.

Lógicamente, en los demás sectores en los que existen deberes de colaboración sobre el sector privado, aunque no se recoja una limitación semejante, tampoco puede exigirse una cooperación desproporcionada. Por ello, lo mencione o no el legislador de manera explícita, lo cierto es que ese límite opera también en los deberes de colaboración establecidos en los ámbitos de la intervención de las comunicaciones, de los registros remotos y de la conservación de los datos.

Su contenido, eso sí, deberá ser determinado caso por caso tras un juicio de ponderación, pues las condiciones para afirmar la desproporción varían de un ámbito a otro. De este modo, para calibrar el contenido de la carga, deberá tenerse en cuenta aquello que se exige al sujeto llamado a colaborar y lo que implica en concreto para él. Y para determinar si resulta o no desproporcionado, deberá compararse el contenido de la obligación con las circunstancias que rodean la investigación a las que hace referencia el ya mencionado artículo 588 bis a 5, entre las que ocupan un lugar destacado las alternativas de que dispone el investigador criminal para hallar la información que busca, la gravedad del delito que se intenta esclarecer(37), la fiabilidad de los indicios existentes(38) y lo que se pretende lograr con la investigación.

---

(37) Especialmente esclarecedor resulta a este respecto el AAP de Tarragona 1004/2006, de 19 de diciembre que, tras analizar la excepcionalidad, necesidad e idoneidad de la medida, considera que no es proporcionada al sacrificio de derechos que comporta por razón del delito investigado «ya que los resultados que se obtendrían, en su caso, serían de unas tarjetas SIM que se han activado con el teléfono móvil sustraído, lo que supondrá investigar a personas que pudieron haber adquirido el terminal en algún establecimiento de segunda mano o a distancia y, en cualquier caso, a falta de todo otro indicio de participación, no podría imputárseles más que un delito de receptación, que no cumple el mínimo penológico de los tres años de prisión (ya que el artículo 298 del Código Penal castiga la receptación con la pena de seis meses a dos años)» (FJ 3).

(38) Recientemente, la STS 1117/2022, de 15 de marzo (FJ 2), recuerda de nuevo que «han de excluirse las investigaciones meramente prospectivas, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional; exclusión que se extiende igualmente a las hipótesis subjetivas y a las meras suposiciones y conjeturas, pues si el secreto pudiera alzarse sobre la base de esas hipótesis quedaría vacío de contenido (SSTC 49/1999;

La razón que explica por qué el legislador ha omitido esta referencia en los restantes deberes de colaboración reside en el accidentado camino recorrido por estos deberes en su regulación normativa(39). Así lo prueban los sucesivos cambios de ubicación y de contenido. No olvidemos que el deber de colaboración ha mudado de ubicación en varias ocasiones: mientras el Borrador de Anteproyecto del Código Procesal Penal de diciembre de 2012 lo situaba en los registros remotos de equipos informáticos, el primer Borrador del Anteproyecto lo trasladó al registro de dispositivos de almacenamiento masivo, para ser recolocado de nuevo con el Anteproyecto definitivo en el ámbito de los registros remotos. Su contenido ha resultado asimismo variable, pues en un principio se hablaba de un genérico deber de colaboración del responsable del sistema de información y, posteriormente, se ha tratado de concretar el contenido de esas conductas de colaboración.

Por eso, no resultan convincentes los argumentos proporcionados por la Circular de la FGE 5/2019, de 6 de marzo, sobre registro de dispositivos y equipos informáticos que, cumpliendo con esa máxima de hacer de la necesidad virtud, viene a afirmar que en realidad ésta es una regulación deseable y adecuada.

En efecto, de acuerdo con esa interpretación de la Fiscalía General del Estado, la omisión de toda referencia al principio de proporcionalidad en el caso del registro remoto obedece, no tanto a la voluntad del legislador de introducir una excepción en este ámbito como al intento de advertir que, en tales casos, para que sea considerada excesiva, la carga ha de ser más onerosa que en el supuesto de registro de dispositivos de almacenamiento masivo(40). Se pretende justificar así esta falta con el argumento de que en el marco de los registros a distancia «la Ley ha querido limitar las excepciones al mínimo imprescindible». No obstante, no parece que se pueda disculpar semejante omisión alegando que las excepciones son mínimas, puesto que sean éstas pocas o muchas, el respeto al principio de legalidad obliga mencionarlas expresamente. No en vano, el Consejo de Estado en su Informe se mostró favorable a recoger las excepciones de manera expresa.

Por lo demás, estamos de acuerdo con las afirmaciones de la FGE relativas a la mayor intensidad de los deberes de colaboración en el

---

166/1999; 171/1999; 299/2000; 14/2001; 138/2001; 202/2001; 167/2002; 261/2005; 136/2006; 253/2006; 148/2009; 197/2009; 5/2010 y 26/2010)».

(39) Véase, con detalle, Rodríguez Lainz, J. L. en la Encuesta Jurídica del Sepín de octubre de 2016, *op. cit.* (último acceso 6/3/2022), y el mismo en: «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?», *op. cit*., p. 9.

(40) Esta interpretación es acogida por Martínez Atienza, G.: *Investigación tecnológica en los ciberdelitos*, Ediciones Experiencia, 2021, p. 161.

caso de registros remoto que los existentes para el ámbito de los registros directos. En tal sentido, la creación y envío de troyanos para permitir el registro a distancia constituyen, por sí mismas, tareas arduas y de gran complejidad técnica. Y estas mayores exigencias se corresponden, de acuerdo con la Circular 5/2019 FGE, con la especial gravedad de los delitos en los que está permitido el registro remoto(41), con «la mayor dificultad que entrañan los registros remotos», que «exige, también, mayores herramientas que posibiliten su desarrollo».

Sin embargo, tampoco consideramos que esta especial intensidad justifique la omisión a la referencia a la carga desproporcionada, pues precisamente la mayor –o la única– virtud de los términos vagos, como éste, la constituye su capacidad de adaptación a distintos supuestos. Incluirlo aquí hubiera sido lo adecuado, justamente porque el carácter indeterminado del calificativo «desproporcionada» se amolda a las distintas intensidades del deber de colaboración de que se trate: para afirmar la desproporción, si la intensidad es mayor, la carga deberá ser mayor también.

Actualmente, y recapitulando la información que hemos expuesto anteriormente, el deber de colaboración se ha sustanciado en la siguiente redacción: en el ámbito de la interceptación de las comunicaciones se exige prestar «la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones» (art. 588 ter e.1 LECRim); en el caso del registro de dispositivos de almacenamiento masivo se obliga al sujeto requerido a que «facilite la información que resulte necesaria» (art. 588 sexies c.5 LECrim); y, por último, en marco del registro remoto, se establecen, a su vez, dos tipos de deberes de colaboración de diversa intensidad.

En este registro a distancia existe un deber que podemos calificar de mayor intensidad, que es el de «facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema» incluyéndose también el deber de «facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización», que rige para los prestadores de servicios y personas señaladas en el artículo 588 ter e LECrim –es decir, los mencionados en la interceptación de las comunicaciones– y

(41) Se limita a los delitos tasados en el apartado 1 del artículo 588 septies: a) Delitos cometidos en el seno de organizaciones criminales; b) Delitos de terrorismo; c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente; d) Delitos contra la Constitución, de traición y relativos a la defensa nacional; e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

los titulares o responsables del sistema informático o base de datos objeto del registro (art. 588 septies b.1 LECrim).

Y junto a él se regula otro deber colaboración de menor intensidad, consistente en que se «facilite la información que resulte necesaria para el buen fin de la diligencia», y que es impuesto a «cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el dispositivo» (art. 588 septies b. 2. LECrim). Una última referencia a los deberes de colaboración es la contenida en las medidas de aseguramiento (art. 588 octies LECrim). En este precepto, dedicado a la orden de conservación de datos, se permite al Ministerio Fiscal o a la Policía Judicial requerir «a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición» hasta obtener la autorización judicial correspondiente para su cesión.

En general, esa llamativa falta de regularidad se ha visto reflejada también en otras partes del articulado. Por ejemplo, cabe destacar la desigualdad del legislador a la hora de establecer deberes de sigilo acerca de las actividades que son requeridas por las autoridades, pues sí lo ha exigido en el ámbito de la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter e.2 LECrim), en el registro remoto (art. 588 septies b.3 LECrim) y en la orden de conservación de datos (art. 588 octies LECrim), pero no en el registro físico de dispositivos de almacenamiento masivo, a pesar de que eximir del deber de guardar sigilo a estos destinatarios del deber de colaboración no tendría ninguna lógica.

Curiosamente, en lo único en lo que ha habido uniformidad, puesto que se repite en todos los ámbitos con cierto paralelismo(42), ha sido en la amenaza de incurrir en un delito de desobediencia del artículo 556.1 CP, a pesar de que, precisamente, gran parte de los destinatarios del deber de colaboración no pueden responder por este delito, por la sencilla razón de que no es uno de los contemplados en

(42) Tras hacer caso esta vez a la recomendación del Consejo de Estado en su Informe al Anteproyecto de la LECRim y corregir consiguientemente la omisión a la referencia a la posible comisión de un delito de desobediencia. Véase el apartado h) dedicado a la colaboración de terceros, disponible en https://www.boe.es/buscar/doc.php?id=CE-D-2015-97 (último acceso 3/7/2021). En el Anteproyecto de Ley de Enjuiciamiento Criminal, aprobado por Consejo de Ministros el 24 de noviembre de 2020, desaparecen la mayor parte de las referencias a la desobediencia y se mantiene exclusivamente en el registro de dispositivos de almacenamiento masivo de información del artículo 428 del Anteproyecto.

el catálogo *numerus clausus* de infracciones penales susceptibles de generar responsabilidad penal de la persona jurídica.

Con estas consideraciones queremos, en definitiva, poner de manifiesto cierta falta de celo por parte del legislador, tanto a la hora de regular la excepción de la desproporción de la carga, como al desarrollar las cuestiones relacionadas con los deberes de colaboración. Aunque, desde luego, la redacción dista mucho de ser perfecta, no parece, sin embargo, que esa falta de precisión obedezca tanto a una actitud despreocupada o desidiosa, como al hecho de que se trata de una materia compleja y excesivamente técnica, ajena al ámbito en el que tradicionalmente se desenvuelve el jurista y que constituye, por lo demás, una materia enormemente cambiante. Tratando de huir de una excesiva inconcreción, el legislador dedica a cada ámbito en el que puede obtenerse la prueba digital una regulación separada, con una redacción seguramente mejorable.

Más adecuado hubiera sido, parece, que el legislador hubiera establecido un deber de colaboración unitario –añadiendo también la excepción de la desproporción de la carga– en las disposiciones comunes que actúan como principios rectores –esto es, en artículos 588 bis a al 588 bis k LECrim (43)–, y que allí también hubiera regulado tanto las excepciones al deber de colaborar, como el deber de guardar silencio y la posibilidad de incurrir en delito de desobediencia.

Parece, pues, claro que la selección de conductas en las que se materializan los deberes de colaboración responde a un intento por parte del legislador de concretar tareas para no apartarse más de lo debido del principio de legalidad, y no a la voluntad de limitar a un mero deber de facilitación de información la colaboración de quien puede hacer mucho más que eso. Más bien, las tareas que se mencionan son aquellas que se consideraban posibles de acuerdo con el estado de la evolución tecnológica del momento de su redacción. Consideramos que, en definitiva, lo que ha buscado el legislador ha sido, simplemente, permitir al investigador público exigir la ayuda de cualquiera dentro de lo razonable.

Realmente, el legislador podía haber regulado las normas con mayor precisión y haber contado, además, con un mayor apoyo por parte de expertos en el mundo informático(44). Porque hay que reco-

(43) En este sentido, ya SÁNCHEZ MELGAR, J. en la Encuesta Jurídica publicada por la editorial Sepín en octubre de 2016, *op. cit.* (último acceso 6/3/2022).

(44) En este sentido, resulta especialmente crítico RUBIO ALAMILLO que afirma que «observando el texto redactado del nuevo articulado de la Ley de Enjuiciamiento Criminal, se puede deducir con facilidad que el Gobierno que, conforme a nuestro ordenamiento jurídico, ha liderado la reforma, no ha estado correctamente asesorado

nocer cierta mala fortuna en la elección de los verbos en los que se concreta esa colaboración, cuando el destinatario de la obligación es «cualquier persona que conozca» el funcionamiento del sistema o las medidas, mientras que cuando los verbos han sido los adecuados (facilitar la colaboración precisa y prestar la asistencia necesaria), entonces lo que ha fallado ha sido la elección de los sujetos.

Por estos motivos, decimos, se impone una interpretación extensiva, pues carecería de toda lógica que las empresas tecnológicas no se sitúen en el elenco de sujetos a los que se exige una colaboración más amplia, como tampoco tendría sentido que se establecieran obligaciones distintas dependiendo de si el registro del mismo dispositivo se lleva a cabo de manera directa o remota.

C) **Criterios para determinar la desproporción de la carga**

La referencia al carácter desproporcionado de la carga tiene su origen en el Convenio de Budapest, pues ya su artículo 19.4 establecía la obligación de que la colaboración exigible se moviera «dentro de lo razonable». Se citaba, asimismo, como ejemplo de irrazonabilidad en la exigencia de la divulgación de una contraseña u otra medida de seguridad, que la misma «pudiera poner en peligro injustificadamente la vida privada de otros usuarios o de otros datos cuya revisión no ha sido autorizada. En tal caso, el suministro de la información «necesaria» podría consistir en la revelación, en una forma que sea comprensible y legible, de los datos que realmente andan buscando las autoridades competentes»(45).

El criterio de la proporcionalidad constituye, por lo demás, uno de los principios rectores comunes a todas las medidas de investigación tecnológica recogidos en el artículo 588 bis a.2 LECrim junto con los principios de especialidad, idoneidad, excepcionalidad y necesidad. Su aplicación implica que, a la hora de decidir una determinada medida de investigación, deban ser tenidas en cuenta tanto las circunstancias del caso, como los intereses en juego y los derechos afectados, de forma que de la adopción de esa medida resulte siempre un saldo favorable al interés público y a los terceros. De este modo, las resoluciones judiciales que permiten la adopción de una medida o su

---

por los profesionales que mejor conocen la Informática y las redes, es decir, por Ingenieros e Ingenieros Técnicos en Informática». Véase RUBIO ALAMILLO, J.: «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *op. cit*., p. 4.

(45) Véase el Informe explicativo del Convenio sobre la Ciberdelincuencia del Comité de Ministros del Consejo de Europa en su 109.ª reunión (8 de noviembre de 2001), p. 5, disponible en: https://rm.coe.int/16802fa403 (último acceso 5/1/2022).

prórroga han de referir todos los elementos indispensables para realizar el juicio de proporcionalidad y hacer posible su control posterior(46).

Por lo tanto, como límite objetivo al deber de colaboración el legislador ha vuelto a optar por el principio de proporcionalidad, un criterio valorativo e indeterminado que deberá ser precisado caso por caso. A pesar de que una desproporción como esa pueda utilizarse en la práctica para excluir del deber de colaborar a determinados sujetos que el legislador olvidó de excepcionar incomprensiblemente del círculo de obligados a colaborar con el investigador público, no puede limitarse solo a esto la desproporción, pues el legislador no estaba pensando en ellos cuando la introdujo(47).

Por lo que respecta a los criterios para determinar la proporcionalidad de la carga que supone la colaboración, resulta muy esclarecedor el contenido del apartado 5.º del artículo 588 bis a LECRim, artículo que, como señala Álvarez Sánchez de Movellán(48) constituye solo «la punta de lanza del principio» de una construcción jurídica, la de la investigación tecnológica, «que respira proporcionalidad por todos sus poros».

Primero, se afirma, de acuerdo con un criterio asentado ya en nuestra doctrina(49) y jurisprudencia(50)– que la medida será proporcionada cuando «el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros». No puede perderse de vista que el derecho del propietario del *hardware* o *software* cuyo sacrificio se discute es uno ordinario: el de la propiedad privada(51). A ello se añade –y la determinación de este criterio constituye una auténtica novedad– que «la

(46) Por todas, STS 1024/2022, de 15 de marzo (FJ 1.º).

(47) Analicé esta posibilidad, propuesta por la Circular FGE 5/2019, en «El investigado o encausado, el abogado y el pariente como sujetos excepcionados del deber de colaborar en la obtención de la prueba digital», *op. cit.*, pp. 27 y 39.

(48) Álvarez Sánchez de Movellán, P.: «Las nuevas medidas de investigación tecnológica y la enésima invocación al principio de proporcionalidad», *Justicia: Revista de Derecho procesal*, 2018, núm. 1, p. 105.

(49) Véase al respecto Bachmaier Winter, L.: «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *op. cit*., p. 15.

(50) Como ya estableció la STC 207/1996, de 16 de diciembre, (FJ 3) y repite, entre otras, la STC 70/2002, de 3 de abril (FJ 10) «que se deriven de su aplicación más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o intereses en conflicto o, dicho de otro modo, que el sacrificio impuesto al derecho fundamental no resulte desmedido en relación con la gravedad de los hechos y las sospechas existentes (juicio de proporcionalidad en sentido estricto)».

(51) Así lo destaca Perals Calleja en la Encuesta Jurídica publicada por Sepín en octubre de 2016, *op. cit*, p. 4 (último acceso 6/3/2022).

valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.»

Por lo tanto, para la determinación del contenido de la carga habrá de tenerse en cuenta, en primer lugar, el esfuerzo y dedicación que implica la colaboración para el sujeto requerido –que no será igual, lógicamente, tratándose de un particular o una gran empresa–. Es decir, ha de ser objeto de ponderación tanto lo que el sujeto ha de hacer como lo que ha de dejar de hacer para prestar la ayuda solicitada. En segundo lugar, habrá que calibrar los costes económicos y de otra índole que la colaboración supone para el sujeto en cuestión, especialmente los relativos a los sacrificios de la propiedad intelectual e industrial. Aquellos que resulten cuantificables podrán ser resarcidos de acuerdo con lo establecido en el artículo 17.1 LOPJ(52).

Un problema mayor plantea la indemnización del riesgo o coste reputacional, que puede generar pérdidas, a veces muy cuantiosas, en distintos ámbitos (de negocio, de valor bursátil, de mercado, etc.), pero que al tener un carácter indirecto resultan muchas veces de difícil cuantificación y, por tanto, de complicada reparación. Respecto a esta materia nos gustaría destacar que, en el caso de las multinacionales que se niegan a colaborar con el investigador criminal, –particularmente sonoro ha sido el enfrentamiento de *Apple* con el FBI–, llama poderosamente la atención que la facilitación del acceso a un dispositivo dirigido a la evitación de la muerte de personas juegue en contra y no a favor de su buen nombre. En concreto, a propósito de la negativa de la empresa de Cupertino tras las peticiones del FBI, una encuesta realizada por la CBS(53) arrojó un saldo favorable a la colaboración, aunque con un margen pequeño. Sin embargo, aunque aceptáramos como válida la premisa de que *Apple* sufriría un daño reputacional si colaborara activamente con los servicios de investigación estatales, entonces ese mismo daño podría afirmarse también cuando se pone en conoci-

(52) Artículo 17 LOPJ: «1. Todas las personas y entidades públicas y privadas están obligadas a prestar, en la forma que la ley establezca, la colaboración requerida por los Jueces y Tribunales en el curso del proceso y en la ejecución de lo resuelto, con las excepciones que establezcan la Constitución y las leyes, y sin perjuicio del resarcimiento de los gastos y del abono de las remuneraciones debidas que procedan conforme a la ley».

(53) En la encuesta participaron más de 1.000 ciudadanos. Un 50% se mostró favorable a la colaboración con el FBI y un 45%, reacio. Pueden verse los datos en https://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone/ (último acceso 3/2/2022).

miento del público general que existe una empresa alternativa, como la israelí *Cellebrite*, capaz de proporcionar acceso a un dispositivo.

En todo caso, si se apreciara la existencia de un daño reputacional, debería valorarse negativamente el hecho de que *Apple*, más allá de defender a ultranza la privacidad, haya construido su reputación precisamente sobre el descrédito del mismísimo FBI. Resultaría paradójico que un Estado tuviera que indemnizar a una empresa por afectar la fama de un producto, cuando la empresa no solo ha erigido su prestigio precisamente sobre el desafío continuo a la investigación criminal y a los organismos que se encargan de llevarla a cabo, sino que se ha ocupado, además, de publicitar el reto.

Con independencia de estas reflexiones, para determinar el interés público, al otro lado de la balanza se situaría, en primer lugar, la gravedad del hecho. En dicho parámetro deberá calibrarse, primero, la severidad de la pena prevista para el delito que se está investigando. Éste constituye un criterio tenido en especial consideración por parte del legislador de las nuevas tecnologías, puesto que tanto la interceptación de las comunicaciones telefónicas y telemáticas como el registro a distancia está reservado para un listado de delitos considerados de especial gravedad.

Ello es así en teoría, porque en ambos casos se incluye un inciso final que abre el abanico a otros delitos que no tienen que ser graves. Así, recordemos, que en el caso de la interceptación de las comunicaciones, según el artículo 583 ter a, la autorización para llevarla a cabo queda reservada a los delitos contemplados en el artículo 579.1 LECrim, es decir, a los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, a cometidos en el seno de un grupo u organización criminal, a los delitos de terrorismo y, además, a los «delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación». Esa misma referencia se contiene en los delitos en los que está permitido el registro remoto. En el listado se incluyen los delitos cometidos en el seno de organizaciones criminales, los delitos de terrorismo; los delitos cometidos contra menores o personas con capacidad modificada judicialmente y los delitos contra la Constitución, de traición y relativos a la defensa nacional, pero se añade también una última categoría idéntica referida a «delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación».

Estos añadidos han sido objeto de duras críticas por parte de distintos autores(54), puesto que el hecho de que en la comisión se empleen medios informáticos o telemáticos nada indica acerca de la gravedad del delito. Así, Zaragoza Tejada(55) recuerda la incongruencia existente en el hecho de que no puedan investigarse a través de estas medidas delitos como un homicidio, un asesinato o una agresión sexual, pero sí otros delitos menores como la estafa informática, y propone una regulación similar a la del Anteproyecto del 2013, que preveía la creación de *softwares* para los delitos graves y, además, para aquellos en los que el uso de *softwares* fuera necesario para su esclarecimiento. A esta particularidad tendremos ocasión de pronunciarnos más adelante.

En cualquier caso, para determinar la gravedad del hecho deberá ser tenida en cuenta también su trascendencia social(56). La sensibilidad de la sociedad con respecto a determinados delitos habla a favor de la utilización de técnicas de investigación más invasivas. Y a estos criterios de la gravedad y de la necesidad, debe añadirse otro: la finalidad que pretende alcanzarse con la información que se obtenga. No será lo mismo, por ejemplo, tratar de condenar a un sujeto que intentar impedir la comisión próxima de un atentado terrorista, debiendo ser valorada también la urgencia, pues el recurso a las empresas alternativas requiere normalmente de un plazo de tiempo superior por la falta de familiaridad con el producto.

Para que el saldo arrojado sea favorable al interés público también resultará fundamental la solidez de los indicios existentes. El principio de especialidad requiere que la medida se adopte para la investigación de un delito en concreto. Por lo tanto, la medida solo podrá acordarse para investigar un delito de cuya comisión se tienen sospechas fundadas, quedando vetada cualquier diligencia restrictiva de derechos fundamentales adoptada en una situación que se asemeje a eso que en terminología anglosajona se denomina una *fishing expedition*: una investigación prospectiva realizada sin verdaderos indicios de la existencia de un delito. Como recuerda la STS núm. 404/2016, de 11 de mayo(57), se requieren «indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales

(54) Ya el propio Rubio Alamillo, J.: «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *op. cit.* pp. 6 y 10.

(55) Véase Zaragoza Tejada, J. I.: «El registro remoto de equipos informáticos», *op. cit*., p. 460.

(56) La vinculación de la trascendencia social con el ámbito tecnológico de producción se afirma en el AAP de Madrid 131/2015, de 25 de febrero (RJ 3).

(57) STS núm. 404/2016, de 11 de mayo (FJ 4).

que se exigen para el procesamiento»(58). Para la validez de esos indicios se requiere una objetividad que, de acuerdo con la argumentación de la Sentencia, puede afirmarse cuando se dan tres requisitos: «1.º) ser accesibles a terceros, sin lo cual no serían susceptibles de control; 2.º) proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, y 3.º) no consistir en valoraciones acerca de la persona»(59).

En definitiva, tendrán que aplicarse los principios rectores comunes a todas las medidas de interceptación y registro adaptándolas en este caso, más allá de a una posible vulneración del derecho al secreto de las comunicaciones y a la intimidad, a una posible vulneración del derecho a la propiedad industrial e intelectual.

D) **La creación de una puerta trasera como forma de colaboración exigible**

Por lo que respecta a la cuestión concreta de si ha de considerarse desproporcionado obligar al requerido a desvelar un secreto industrial y/o a diseñar una aplicación que permita forzar la clave de acceso, lo cierto es que existen a este respecto opiniones muy diversas y plagadas de matices. Basta remitirnos a la encuesta de la Editorial jurídica Sepín del año 2016, que muestra cómo entre las opiniones positivas y desfavorables, que desarrollaremos más abajo, se abre un abanico de criterios intermedios que condicionan la posibilidad a la comisión de determinados delitos o al cumplimiento de determinados requisitos(60).

Frente a esta disparidad de criterios, la Circular 5/2019 resulta clara: mientras que en el caso de registros remotos sí puede requerirse la realización de un trabajo en sentido amplio que permita la realiza-

(58) Sobre la importancia de los indicios resulta especialmente relevante la STC 49/1999, de 5 de abril y más recientemente las SSTC 136/2000, de 29 de mayo y 253/2006, de 11 de septiembre y 145/2014, de 22 de septiembre.

(59) STS núm. 404/2016, de 11 de mayo (FJ 4).

(60) Pueden verse distintas opiniones de Magistrados, Fiscales y abogados en la Encuesta Jurídica publicada por *Sepín* en 2016. A favor, Rodríguez Láinz, J. L. (el mismo en «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?», *op. cit.,* p. 11) y Velasco Núñez; en determinados supuestos, Perals Calleja, J. y Santaló Junquera, J. I.; y en contra de esta opción se manifiestan Moreno Verdejo, J., Sánchez Melgar, J. y Narváez Rodríguez, A., disponible en https://sepin.es/cronus4plus/documento/VerDoc.asp?dist=55&referencia=SP%2FDOCT%2F21122&cod=0JP2JP1Cv0FF1T10Vb0FP1%24v0GC0Fa1yB0G909P17P0Vf08A1ek1S308A1vd1yi05u1dF1Dk0Ha1%3DP01b0Fa17T1DT0Fk1C50Gz0Fa1Aa01f0Ha1Aa1Dg0Fa1C42AA0G%5F1C51Cv0FF0yg0HL0GB0Oq01E#25605745 (último acceso 6/3/2022).

ción de una diligencia de investigación, en los registros directos la colaboración activa exigible queda limitada a un deber meramente informativo consistente en proporcionar las claves de acceso o indicar la ubicación de los datos. Por lo tanto, si se planteara un caso similar al del conflicto entre *Apple* y el FBI estadounidense en territorio español, la argumentación de la FGE se situaría del lado de *Apple*, que podría legítimamente, de acuerdo con este criterio, negarse a introducir *backdoors* en su propio sistema.

Sin embargo, nosotros no podemos estar de acuerdo con este criterio. Consideramos que la respuesta no puede ser en todo caso negativa ni tampoco hacerla depender del tipo de registro que se vaya a llevar a cabo. Además, semejante tesis derivaría de una interpretación literal del artículo 588 sexies c.5 LECrim de la que discrepamos. De acuerdo con ese criterio favorable a la literalidad, puesto que ante el registro de un dispositivo de almacenamiento masivo el legislador únicamente se refiere a la posibilidad de obligar a una persona a que «facilite la información necesaria», todo lo que exceda esa facilitación de información –en el sentido de transmitir los conocimientos que ya se tienen– ha de considerarse una carga excesiva.

Por lo tanto, el deber de colaboración establecido por el legislador hace referencia a la facilitación de la información necesaria para el registro, pero no alcanza al desarrollo de actividades o trabajos tendentes a posibilitar el registro, como sería, por ejemplo, la creación de programas informáticos específicos destinados para ello. De este modo, se entiende que la carga sería, sin duda, desproporcionada, como decimos, cuando se obligara al requerido a desvelar un secreto industrial, o a diseñar una aplicación que permitiera forzar la clave de acceso en el caso de un registro directo. Nosotros nos mostramos contrarios a ese entendimiento literal del precepto, como expondremos en el siguiente apartado.

En todo caso, incluso con una interpretación amplia de la colaboración exigible en el registro directo, podría entenderse que la carga sería en todo caso excesiva si se diera por válida la razón principal de la negativa de *Apple*. La empresa norteamericana auguraba grandes calamidades con la creación de la puerta trasera: ese mecanismo de acceso acabaría cayendo en las manos erróneas con toda seguridad e incluso en las manos correctas sería objeto de un uso ilimitado y abusivo.

En la misma línea argumental se pronunció el alto Comisionado de las Naciones Unidas para los Derechos Humanos, el jordano Zeid Ra'ad Al Hussein, que afirmaba(61) que «las autoridades corren el riesgo de abrir una caja de Pandora con implicaciones extremadamente

(61) Pueden leerse sus declaraciones en: https://www.elmundo.es/tecnologia/2016/03/04/56d9a352ca474185168b45dc.html (último acceso 10/3/2022).

perjudiciales para los derechos humanos de millones de personas», puesto que ceder a las pretensiones del FBI «sería un regalo para regímenes autoritarios, así como para delincuentes informáticos». Parece evidente que una discusión no puede desarrollarse en términos absolutos de «todo acceso» o «ningún acceso». Ningún derecho –y, por tanto, tampoco el relativo a la intimidad, a la protección de datos o al mismísimo secreto de las comunicaciones– tiene un carácter ilimitado.

No resulta convincente la razón proporcionada por el CEO de *Apple*, Tim Cook, arguyendo que conceder al FBI una puerta trasera supone poner en peligro la seguridad de los usuarios, puesto que no se puede controlar que se vaya a dar el uso para la que fue creada. Bastaría crear un procedimiento que proporcione las suficientes garantías. Y desde luego, uno en el que media una orden judicial y la intervención de los cuerpos de seguridad de un Estado de Derecho ha de tenerse por suficientemente garantista. Además, ni siquiera resultaría indispensable que *Apple* proporcionara la forma de acceder; bastaría con que proporcionara la información que le es requerida. En este sentido, ya el Convenio de Budapest, como hemos visto, preveía que en aquellos casos en los que exigir la facilitación de contraseñas o métodos de desbloqueo resultara peligroso, entonces podía el obligado dar cumplimiento al mandato de colaboración simplemente proporcionando los datos concretos.

Por lo demás, resultan fácilmente imaginables situaciones graves en las que obligar a diseñar una aplicación o incluso a revelar un secreto industrial no suponga una carga susceptible de ser calificada como desproporcionada: un caso en el que se sepa que un terrorista(62) que está en paradero desconocido va a cometer un atentado de grandes dimensiones. Acudir a una empresa alternativa no es una opción, debido a la urgencia en obtener la información. En tal supuesto, podría exigirse a cualquier fabricante que permitiera acceder a su contenido por la sencilla razón de que, por muy grave que fuera el supuesto daño reputacional y económico, la balanza se inclinaría siempre a favor de la vida y la integridad de las personas.

(62) En este sentido, Martínez Atienza afirma que «en los delitos especialmente graves, en los que esté comprometida la vida de alguna persona o la seguridad pública (como ocurriría en los delitos de terrorismo), deberán ceder, de ordinario, los intereses de la persona requerida. Por el contrario, cuando se trate de delitos de menor importancia o cuando los datos que el registro pueda proporcionar a la investigación no sean especialmente determinantes, deberán valorarse con mayor intensidad los intereses del requerido». Véase Martínez Atienza, G.: *Investigación tecnológica en los ciberdelitos*, *op. cit*., p. 151.

6. OBSERVACIONES ACERCA DE LA EXPRESIÓN «FACILITAR INFORMACIÓN»

A) **Interpretaciones posibles acerca del deber de facilitación de información**

Tal y como venimos señalando, en la Circular 5/2019 la Fiscalía General del Estado se muestra favorable a una interpretación literal de la expresión «facilitar información», empleada en los artículos 588 sexies c y 588 septies b LECrim.

De este modo, entiende que esa colaboración intelectual que supone la facilitación de información constituye la única colaboración exigible, con independencia del sujeto de que se trate, cuando el registro es directo. Y constituye, asimismo, la colaboración exigible en el registro a distancia, salvo que el destinatario de la obligación sea un prestador de servicios, en cuyo caso se puede exigir una colaboración más amplia. De acuerdo con la interpretación de la FGE, fuera de estos casos de colaboración más amplia de los prestadores de servicios, en los registros de los dispositivos «lo único que podrán ordenar las autoridades o agentes encargados de la investigación será la facilitación de la información, pero nada más»(63).

Así, solo sería posible exigir el suministro de datos, como el relativo a las claves de acceso o la ubicación de datos o el asesoramiento técnico, quedando excluido el que suponga la revelación de un secreto industrial, pues ello resultaría vetado por aplicación de la segunda parte de la regulación del deber de colaboración, referido a la carga excesiva. Por lo tanto, aunque según esta interpretación sí sería posible ordenar a una empresa tecnológica que revelara cómo se crea una puerta trasera (pues entraría dentro del concepto «facilitar información»), ello tendría que ser rechazado al suponer esa información una lesión de un secreto industrial, calificable como carga desproporcionada.

En tal sentido, se afirma en la Circular 5/2019 que debería ser considerada excesiva, en principio, «la facilitación de información que supusiera desvelar secretos industriales que pudieran perjudicar una actividad empresarial del afectado, como resultaría de facilitar información sobre los sistemas de seguridad de un determinado teléfono o dispositivo informático»(64).

---

(63) Véase el apartado 3.7 de la Circular 5/2019, disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244 (último acceso 13/2/2022).

(64) Ibídem.

En una línea semejante a la de la FGE se sitúan las posiciones de Jaime Moreno Verdejo y de Julián Sánchez Melgar(65), para quienes no es posible obligar a crear un programa que permita el acceso, pero sí obligar a que se proporcione la información de que se disponga. Moreno Verdejo considera que resulta una carga desproporcionada pedir al fabricante que modifique su producto y desdibuje una de sus características esenciales, y en parecido sentido Sánchez Melgar rechaza la posibilidad de exigir la elaboración de un programa *ad hoc*, pero no facilitar la información que se posea siempre y cuando no constituya una carga desproporcionada. Por último, el magistrado Narváez Rodríguez(66) también rechaza esta modalidad de colaboración, si bien lo hace de manera especialmente enérgica compartiendo las mismas preocupaciones de la empresa *Apple* cuando manifestó su negativa a colaborar con el FBI.

Frente a esta postura, se alza otra opinión que se muestra favorable a la posibilidad de exigir la creación de esos *softwares* denominados puertas traseras. Tal sería el parecer, por ejemplo, de Rodríguez Lainz(67), quien, partiendo de la calificación de *Apple* como prestadora de servicios por su control sobre *iTunes* y *iCloud*, destaca lo incoherente que resultaría el hecho de poder exigir a *Apple* la creación de una puerta trasera para un registro remoto, pero no para un registro directo. También a favor de permitir que se exija ese tipo de colaboración parece posicionarse tanto el Magistrado Velasco Núñez, aunque recuerda que solamente se tolera para que se facilite la información necesaria, como el Fiscal Perals Calleja, que lo admite apriorísticamente sin duda en los delitos de terrorismo y contra la salud pública(68). El abogado Santaló Junquera(69), por su parte, lo admite siempre que medie una autorización judicial. Destaca la opinión de

(65) Texto disponible en: https://sepin.es/cronus4plus/documento/VerDoc.asp?dist=55&referencia=SP%2FDOCT%2F21122&cod=0JP2JP1Cv0FF1T10Vb0FP1%24v0GC0Fa1yB0G909P17P0Vf08A1ek1S308A1vd1yi05u1dF1Dk0Ha1%3DP01b0Fa17T1DT0Fk1C50Gz0Fa1Aa01f0Ha1Aa1Dg0Fa1C42AA0G%5F1C51Cv0FF0yg0HL0GB0Oq01E#256055 (último acceso 6/3/2022).

(66) Ibídem.

(67) Rodríguez Lainz, J. L.: «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información», artículo monográfico, *Revista Sepín*, septiembre 2016, pp. 6-8 (último acceso 27/2/2022).

(68) La opinión de ambos en la Encuesta del Sepín de 2016. Texto disponible en: https://sepin.es/cronus4plus/documento/VerDoc.asp?dist=55&referencia=SP%2FDOCT%2F21122&cod=0JP2JP1Cv0FF1T10Vb0FP1%24v0GC0Fa1yB0G909P17P0Vf08A1ek1S308A1vd1yi05u1dF1Dk0Ha1%3DP01b0Fa17T1DT0Fk1C50Gz0Fa1Aa01f0Ha1Aa1Dg0Fa1C42AA0G%5F1C51Cv0FF0yg0HL0GB0Oq01E#256055 (último acceso 6/3/2022).

(69) Ibídem.

Zaragoza Tejada(70), gran experto en esta materia, para quien la posibilidad de exigir la creación del *softwar*e que permita el acceso derivaría de la necesidad de salvar la incongruencia que supondría «prever esta obligación de colaboración respecto al acceso remoto y no respecto al acceso directo previsto en el artículo 588 sexies» a pesar de que en el registro remoto «la afectación del derecho al secreto de las comunicaciones puede ser, incluso, mayor».

B) **Propuesta de interpretación**

Estimamos adecuado el resultado al que llegan todos los autores favorables a la posibilidad de exigir una colaboración más amplia que la derivada de la interpretación literal de los preceptos. No obstante, en algún aspecto diferimos del camino tomado, puesto que normalmente a esa conclusión se llega tras afirmar la condición de *Apple* como prestadora de servicios. Y, a pesar de que estamos de acuerdo con esa calificación, creemos no puede ser lo determinante para calibrar el grado de colaboración de *Apple*, puesto que aun cuando perdiera el control sobre *iTunes* y sobre *iCloud*, como en su día lo perdió sobre *WhatsApp*, la respuesta ha de ser la misma: quien crea un mecanismo de seguridad inquebrantable para el investigador criminal tiene el deber de garantizar al investigador el acceso a la información cuando ese acceso es la única forma que tiene el investigador de esclarecer el delito.

Como argumentos relevantes consideramos destacable, en primer lugar, el hecho de que, al igual que sucede con el ámbito de aplicación de la excepción relativa a la carga desproporcionada y que vimos en el apartado anterior, tampoco parece que el empleo por parte del legislador de la expresión «facilitar información» sea fruto de una profunda reflexión por su parte que haya desembocado en una intención clara de establecer unos deberes de colaboración distintos dependiendo del tipo de registro.

Una distinción como ésa tendría sentido si, por ejemplo, entre los diferentes tipos de registro se diera en toda circunstancia una sucesión temporal –imaginemos que fuera siempre posible primero llevar a cabo el registro directo del dispositivo, quedando el sujeto requerido únicamente obligado a un mero suministro de información, y que, después, en caso de fallar esta primera opción, fuera posible acudir con la artillería pesada al registro remoto, exigiendo a otros sujetos

(70) Zaragoza Tejada, J. I.: «El registro remoto de equipos informáticos», en *Investigación tecnológica y derechos fundamentales*, *op. cit*., p. 447.

unas tareas colaborativas de mayor calado(71). Pero semejante sucesión temporal no se da. También tendría alguna lógica si, estando limitado –como de hecho está– el registro remoto a delitos de especial gravedad, el registro de dispositivos de almacenamiento masivo estuviera reservado para delitos de menor importancia. Entonces quizás sería admisible entender que en esos delitos menos graves solamente puede exigirse una mera facilitación de información. Pero tampoco esto se corresponde con la realidad de las cosas. Los delitos en los que se permite el registro remoto, que son, en efecto, los de especial gravedad tasados en el apartado 1 del artículo 588 septies a LECrim(72), pueden requerir del registro directo de un dispositivo de almacenamiento masivo como único medio de obtener la prueba digital.

Por lo tanto, y puesto que el poder practicar un registro u otro depende de algo completamente ajeno a la gravedad del delito –y tan aleatorio, por lo demás– como que al dispositivo tenga acceso o no el investigado, –puesto que la instalación del troyano exige la colaboración, involuntaria eso sí, del titular del dispositivo– o como que el dispositivo opere físicamente en manos del investigador público, porque se haya decidido y se haya logrado su incautación y se disponga de la autorización judicial pertinente, no parece razonable vincular el tipo de registro y la clase de colaboración exigible(73).

A ello podríamos añadir que la identificación del deber de colaborar en el caso de los registros directos con un mero suministro de claves y ubicaciones llevaría a un resultado indeseable. Como sabemos, el registro remoto de un dispositivo resulta mucho más agresivo que el

(71) A favor de que la propia ley hubiera establecido esa prelación, permitiendo solo el registro remoto cuando el directo fuera imposible, se manifestaba Bachmaier Winter, advirtiendo del peligro de lo tentador que puede resultar recurrir al registro remoto «más rápido o más económico». Véase Bachmaier Winter, L.: «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *op. cit*., p. 27.

(72) Véase la nota 41.

(73) Acerca de la correlación existente entre el artículo 588 sexies c.5 y el artículo 588 septies b.1, afirma Rodríguez Lainz que «no existe en este sentido una diferenciación de trato que pueda justificar cómo en el último sí pudieran imponerse obligaciones de hacer como la descrita, sin posibilidad además de alegato de excesiva gravosidad, mas no en un supuesto de registro físico en el que nos enfrentamos a idéntico problema. Aparte de los supuestos en que legalmente procede la práctica de la diligencia, la única diferencia existente, de índole exclusivamente técnica, radica en que el acceso en el registro remoto puede enfrentarse a ciertas dificultades cuando la penetración se realiza a través de una vía externa; pero ello no justifica en modo alguno la diferencia de trato». Véase Rodríguez Lainz, J. L.: «Veintiocho discrepancias y refutaciones a las Circulares de la Fiscalía General del Estado de 6 de marzo de 2019 sobre diligencias de investigación tecnológica», *Diario La Ley*, núm. 9416, Sección Doctrina, 16 de mayo de 2019.

registro directo, pues implica que se pueda acceder a un sistema informático sin que lo sepa su titular. En efecto, y como señala la Circular FGE(74), el carácter dinámico de esta medida, frente al estático del registro directo, determina que pueda accederse a una cantidad de datos mucho mayor que en el registro directo y que puedan ser interceptadas las comunicaciones en tiempo real. Y ha de tenerse en cuenta la circunstancia de que el registro remoto es siempre clandestino, puesto que el titular del dispositivo desconoce que se está llevando a cabo.

Por esas razones, las exigencias para el registro remoto son mucho mayores y solo puede llevarse a cabo en uno de los supuestos tasados para los que está prevista. Recordemos también que, a diferencia del registro directo, ni cabe el registro remoto de urgencia convalidado posteriormente por un Juez, ni esa diligencia de investigación es susceptible de ser ampliada a otros sistemas.

Por todo ello, parece que en un escenario hipotético en el que ambos tipos de registro fueran posibles, habría que optar por el registro directo. Sin embargo, parece que los investigadores públicos siempre optarían por el registro remoto, a pesar de su mayor agresividad, y lo harían, además, en aplicación de un principio propio de las diligencias de investigación, como es el de necesidad, puesto que en el caso del registro directo la limitada colaboración exigible no garantiza el acceso al dispositivo investigado.

Otra razón favorable al entendimiento de que toda colaboración es exigible tiene que ver con la regulación introducida por el legislador para el registro remoto de un equipo informático. Como venimos diciendo, este tipo de registro resulta especialmente lesivo, al menos potencialmente, pues permite el recurso a mecanismos-programas espías –*spyware*s, *web bugs*, identificadores ocultos y el recurso al agente encubierto online– que pueden afectar al secreto de las comunicaciones y que resultan gravemente lesivos de la intimidad en la medida en que actúan sin que lo sepa el titular del dispositivo. El legislador ha restringido la utilización de este tipo de registro a delitos especialmente graves, salvo uno: los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. En tal caso no se exige ningún tipo de gravedad.

Ahora bien, con independencia de que esa regulación resulte más o menos deseable, contiene en sí misma una declaración de principios: el legislador no quiere que ningún delito se sustraiga de la investigación criminal por el hecho de cometerse a través de un sistema

(74) Véase el apartado 4.1, Regulación legal, en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244 (último acceso 16/2/2022).

informático. Es ése claramente el motivo por el que no ha exigido una gravedad concreta y mayor: porque no quiere permitir la creación de un ámbito de impunidad para ningún delito.

El motivo por el que se ha hecho uso del término «facilitar información» reside, sencillamente, en que ésa fue la expresión empleada en el Convenio de Budapest. No olvidemos que el artículo 19.4 del Convenio de Ciberdelincuencia hacía referencia al deber de «cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo» a «que facilite toda la información necesaria». El legislador del Convenio de Budapest empleó para regular los deberes de colaboración en el único registro posible entonces –el directo– la fórmula más amplia de la que fue capaz. Carecería de lógica pensar que una década y media después, en pleno auge de los sistemas de seguridad y encriptación, el legislador se fuera a autolimitar el acceso a todas las pruebas digitales contenidas en los dispositivos más comprados del mercado.

En efecto, el legislador se hizo eco de la expresión utilizada en el Ciberconvenio sin plantearse si un entendimiento literal de la expresión «facilitar información» acarrearía posteriormente limitaciones indeseables. No tenía presente entonces ni la versión iOS 8, ni sus sistemas de retardo y autodestrucción. Y es que, en lo que respecta a las nuevas tecnologías, el legislador se debate entre elaborar normas excesivamente imprecisas, o utilizar expresiones llamadas a caducar en un breve periodo de tiempo. A favor de entender que se trata de un descuido habla el hecho de que el legislador se ha preocupado en otros ámbitos de garantizarse el acceso la información en todo caso. Tanto es así que, como vimos, incluye como delitos susceptibles de investigación a través de un registro remoto ni más ni menos que los cometidos en el ámbito informático.

Constituiría una verdadera paradoja que el legislador, tratando de evitar la impunidad de un círculo de delitos, los informáticos, permitiera la agresividad de un registro remoto y a la vez se autodenegara la investigación de todo delito –informático o no– cuando la única manera de esclarecerlo es con la información contenida en un dispositivo –por ejemplo, de *Apple*–, que se encuentra bloqueado.

Otro sector en el que también se ha preocupado de garantizarse el acceso a la información lo constituye el ámbito de las telecomunicaciones. La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en su artículo 39, establece el deber de los sujetos que apliquen a las comunicaciones algún procedimiento de cifrado o codificación la obligación de «entregar aquellas desprovistas de los efectos de tales

procedimientos, siempre que sean reversibles», sin establecer ninguna limitación al tipo de actividades que podía desarrollar el sujeto obligado para cumplir con su deber de entrega. Es más, en el artículo 43, dedicado al cifrado en las redes y servicios de comunicaciones electrónicas, tras permitir, en su apartado 1, que toda información transmitida por redes de comunicaciones electrónicas sea cifrada, se afirma en el apartado 2 que «se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente».

Por lo tanto, la Ley 9/2014 contiene una regulación omnicomprensiva de las obligaciones de quien encripta la información: el sujeto que encripta tiene que desencriptar, pudiendo ser requerido también, ni más ni menos que a facilitar los procedimientos o los aparatos de cifrado. No tiene ningún sentido entender que por las mismas fechas la LECrim haya venido a exigir una colaboración de menor calado que la que se regula en la Ley de Telecomunicaciones: al igual que a quien encripta se le obliga a desencriptar, quien crea barreras para impedir el acceso de terceros a los dispositivos tiene que poder ser obligado a quitarlas, especialmente si solo ese sujeto conoce los vericuetos tecnológicos para hacerlo, o para hacerlo en un tiempo razonable.

Con independencia de lo anterior, sin duda resulta llamativo que en este ámbito de la interpretación del verbo la Circular 5/2015 se ciña al principio de legalidad estricto y entienda que solo puede imponerse lo que gramaticalmente la expresión «facilitar información» permite, mientras que cuando se ha obviado la referencia a la desproporción de la carga como excepción al deber de colaboración en los registros a distancia, proponga esa misma circular hacer una interpretación sistemática mucho más laxa que lo que el sentido literal permite.

A nuestro juicio, se impone aquí una interpretación extensiva. Tres interpretaciones de esta naturaleza serían aquí posibles. Una primera interpretación permitiría entender que la expresión «facilitar información» constituye una concreción meramente ejemplificativa, siendo posible exigir una colaboración que implique otro tipo de tareas, como la creación de una puerta trasera.

A favor de interpretar con amplitud lo que puede exigirse a unos y otros destinatarios habla el Informe del Consejo de Estado, cuando afirma que «estos específicos deberes de colaboración, previstos en atención a la concreta naturaleza de las medidas apuntadas, no son sino manifestaciones de un deber de colaboración que tiene su fundamento último en el artículo 118 de la Constitución y que no limita sus

efectos únicamente a los supuestos indicados sino a cualquiera otros en que puedan resultar necesarios para el éxito de la investigación penal»(75). Una explicación como ésta, situada en las antípodas de lo que propone la FGE, resultaría, quizás, en exceso apartada del principio de legalidad. Otra interpretación factible sería la de entender que esa información que el sujeto está obligado a facilitar y que la LECrim califica de «necesaria» la constituye, sencillamente, aquella que necesita el investigador. Después entraría en juego la consideración de la desproporción de la carga. En este supuesto, no se vulneraría ningún secreto industrial, pues la información acerca de cómo acceder al contenido de nuestro dispositivo quedaría en manos del propio fabricante.

Una última opción, también posible, sería la de conciliar la literalidad que propone la FGE con la interpretación contenida en el Convenio de Budapest. Así, ciñéndonos a la literalidad del precepto, esa «facilitación de información» abarcaría la relativa a cómo crear una puerta trasera. A favor de este criterio habla la redacción del Anteproyecto. En efecto, en el texto del Anteproyecto de LECrim se mantiene esa referencia a la facilitación de la información, pero a diferencia de lo que sucede en el vigente artículo 588 sexies c.5, que contempla el deber de facilitar la información «que resulte necesaria», en el nuevo artículo 428 se precisa un poco más, y se añade «que resulte necesaria para acceder a dichos datos».

En la medida en que, de acuerdo con el estado actual de la técnica, la información almacenada en los servidores de la nube no se corresponde en su totalidad con la contenida en el dispositivo y depende de que el titular realice o no copias en ella, la colaboración que puede requerirse incluye la información relativa a la creación de una puerta trasera (*backdoor*). De este modo, los ingenieros de *Apple* podrían ser obligados a enseñar al investigador público cómo se crea una puerta trasera en su sistema, puesto que eso no deja de constituir un simple suministro de información («para acceder», de acuerdo con el Anteproyecto).

Hasta aquí el razonamiento sería el mismo que el de la Fiscalía General del Estado. A continuación, entraría en juego el criterio de la desproporción de la carga, pero en caso de afirmarse, creemos que ello no puede conducir a la afirmación radical de que cuando no puede exigirse «todo» –es decir, cómo se crea una puerta trasera– entonces

(75) Dictamen del Consejo de Estado al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas. Disponible en: https://www.boe.es/buscar/doc.php?id=CE-D-2015-97 (último acceso 26/2/2022).

necesariamente no puede exigirse «nada». En tal caso, no podrá exigirse la información relativa a cómo acceder al dispositivo, es decir, la que tiene que ver con la creación de la puerta trasera, pero sí podrá reclamarse la entrega de los datos que se buscan. Por lo tanto, de acuerdo con la regulación actual –y con la establecida en el Anteproyecto de LECrim de 2020–, resulta posible obligar a una multinacional a la creación de una puerta trasera. Cosa distinta es que la enorme relevancia de esta forma de investigación, que irá en aumento, aconseje una regulación expresa de este deber de asistencia.

Sea como fuere, y de acuerdo con la regulación vigente, creemos que se dará siempre un elemento que determinará que la carga pueda ser tildada de desproporcionada, aunque ello no constituya más que una concreción de los principios de proporcionalidad y necesidad que rigen en toda la investigación tecnológica. Ese elemento de desproporción no lo constituirá, a nuestro juicio, el peligro para la seguridad de terceros que aduce *Apple* –que no es otro que el que se recogía en el Ciberconvenio cuando se hablaba de la irrazonabilidad de la carga–, puesto que queremos creer que el Estado no haría un uso abusivo e ilegal del acceso. El manejo por parte de un Juez de la información solicitada constituye, en nuestra opinión, garantía suficiente. Tampoco la limitación vendría a nuestro juicio necesariamente por la protección del secreto industrial, puesto que creemos que su sacrificio estaría justificado, al menos, en los delitos especialmente graves y susceptibles de ser investigados a través del registro remoto y en aquellos que, sin ser tan graves, solamente puedan ser investigados a través del registro de dispositivos electrónicos.

La carga sería desproporcionada cuando pudiera ser calificada de innecesaria(76), lo que sucedería siempre en estos casos por la sencilla razón de que existe otra manera menos lesiva de conseguir lo mismo y que permite que el secreto industrial permanezca en la multinacional: que la empresa cree la puerta trasera y sea ella misma la que acceda al dispositivo, facilitando entonces información en el sentido más literal y restringido del término. La precisión establecida en el artículo 428 del Anteproyecto de LECrim, que añade al deber de

(76) Por todas, véase la STS 391/2016, 6 de mayo, que consideró que en la autorización judicial se incumplió el principio de necesidad «toda vez que la solicitud policial se formuló sin haber agotado previamente la práctica de otros medios de investigación que evidenciasen lo imprescindible de la realización de las *escuchas*, así como que tampoco la Resolución autorizante motivaba con suficiencia las razones por las que se produjo el cambio de líneas telefónicas, objeto de investigación, correspondientes a otros titulares distintos del sospechoso inicial» (FD 1.).

facilitación de información que la misma resulte necesaria «para acceder a dichos datos», habla a favor de este entendimiento.

7. CONCLUSIONES

I. Desde el nacimiento de las nuevas tecnologías existe una pugna lógica entre los encargados de la investigación criminal, interesados en acceder al contenido de los dispositivos, y las empresas digitales que, con el objetivo de lucrarse y bajo el pretexto de proporcionar seguridad y tranquilidad a sus usuarios, tratan de dificultar todo acceso no consentido a sus productos. Esta contienda entre el sector público y el privado se ha mantenido hasta tiempos relativamente recientes dentro de lo que podríamos calificar como una desigualdad «aceptable», en la medida en que los investigadores terminaban por lograr su objetivo de introducirse en los dispositivos electrónicos protegidos recurriendo a los denominados «ataques de fuerza bruta». Si bien puede afirmarse con carácter general que la oferta de seguridad ha ido ampliándose paulatinamente en todo el sector tecnológico, el panorama cambiaría particularmente y de manera radical a partir de 2014, cuando *Apple* saca al mercado el sistema operativo iOS 8. Los sistemas de retardo y autodestrucción de datos introducidos con la nueva versión supusieron el fin de la autonomía del investigador criminal, que pasó a necesitar irremediablemente de la colaboración del sector privado para acceder a la información penalmente relevante contenida en los dispositivos electrónicos.

II. Cuatro son los grupos o momentos principales en los que pueden agruparse las obligaciones de cooperar en la investigación tecnológica en la LECrim: la relativa a la intervención de las comunicaciones telefónicas o telemáticas (art. 588 ter e.1 LECrim), la que tiene que ver con el registro de dispositivos de almacenamiento masivo de información (588 sexies c.5 LECrim) la que hace referencia a los registros remotos de equipos informáticos (art. 588 septies b LECrim), y, por último, la que persigue garantizar la conservación de datos (art. 588 octies LECrim). Solamente se hace referencia a la carga desproporcionada como límite objetivo en el registro directo, en el que el deber de colaboración, además, se limita a una facilitación de información. Semejante regulación se mantiene en el texto del Anteproyecto de LECrim de 2020, que precisa en el artículo 428 que esta cooperación ha de ser la «que resulte necesaria para acceder a dichos datos».

III. Creemos que la limitación objetiva de la carga desproporcionada, sucesora de la «razonabilidad» del Convenio de Budapest, constituye una manifestación del principio de proporcionalidad que ha de

regir en todas las medidas de investigación tecnológica, aunque solo se prevea de manera expresa en el registro directo de dispositivos de almacenamiento masivo de datos. La única razón que explica esta regulación asimétrica reside en el accidentado camino recorrido por el deber de colaboración en su evolución normativa y en cierta falta de precisión por parte del legislador a la hora de regular esta materia. No compartimos, por tanto, las explicaciones que proporciona la FGE en la Circular 5/2019, de 6 de marzo, acerca de la omisión a esta referencia en el registro remoto.

IV. La desproporción de la carga constituye un concepto indeterminado cuya concreción exige tener en cuenta las circunstancias del caso. Deberán ser objeto de ponderación, entre otros, el esfuerzo y dedicación que implica la colaboración, los costes económicos y reputacionales que la contribución supone para el sujeto en cuestión, la gravedad del hecho, su trascendencia social, la finalidad que pretende alcanzarse, así como la totalidad de intereses en juego y derechos afectados, de forma que esa colaboración arroje un saldo favorable al interés público y a los terceros. A pesar de que solamente se hace referencia a este límite en el registro de dispositivos de almacenamiento masivo de información, resulta extensible a todos los ámbitos en los que se establecen deberes de colaboración, pues la desproporción de la carga solamente constituye una expresión del principio de proporcionalidad que rige en todas las medidas de investigación, tecnológicas o no, en que se ven afectados derechos fundamentales.

V. Existen diversas opiniones acerca de lo que ha de entenderse por «facilitar información», lo que deriva en distintas concepciones acerca de la asistencia que puede requerirse. A nuestro juicio, de acuerdo con la regulación actual del primer párrafo del artículo 588 sexies c.5 LECrim, la colaboración exigible en el registro directo es cualquiera que permita el acceso a los datos contenidos en el dispositivo. La precisión establecida en el artículo 428 del Anteproyecto de LECrim de 2020, que añade al deber de facilitación de información que la misma resulte necesaria «para acceder a dichos datos», habla a favor de este entendimiento.

VI. Consideramos que la decisión de obligar a las multinacionales a colaborar mediante la creación de puertas traseras (*backdoors*) no puede depender de la condición de la empresa como prestadora de servicios. Exponemos diversos argumentos contrarios al entendimiento de que en el registro directo se impone una colaboración menor que en el registro remoto: ni se da una sucesión temporal entre el desarrollo de ambas medidas ni la posibilidad material de llevar a cabo uno u otro depende de la gravedad del delito. Una diferenciación

como ésta no solo carece de sentido, sino que llevaría a un resultado indeseable: el investigador que pudiera optar entre el registro directo y el remoto elegiría siempre el remoto por carecer éste de limitaciones, a pesar de su carácter más invasivo.

VII. De acuerdo con el estado actual de la técnica, no toda la información contenida en un dispositivo electrónico se encuentra almacenada en los servidores accesibles a través de Internet conocidos como «la nube». Se trata de un tipo de almacenamiento que todavía depende de que el titular realice copias en ella y, aun cuando se realicen las copias, la información no es siempre completa. Por ello, no bastará en todos los casos con que la multinacional proporcione los datos contenidos en la nube, sino que podrá exigirse a las empresas tecnológicas que faciliten la información relativa a la creación de las puertas traseras en tanto en cuanto estas constituyen, a día de hoy, la única forma de acceder al contenido de determinados dispositivos electrónicos.

VIII. En la medida en que exista un medio menos lesivo de acceder a esa información alojada en el dispositivo que permita que el secreto industrial relativo a la puerta trasera permanezca en la empresa, podrá afirmarse la desproporción de la carga y la falta de necesidad de una medida semejante. Por ese motivo, en una segunda valoración, no se impondrá a la multinacional el deber de proporcionar la información relativa a la creación de la puerta trasera –información que, en principio, era exigible–, sino que bastará con que la empresa cree la puerta trasera y sea ella misma la que acceda al dispositivo, facilitando entonces la información allí contenida en el sentido más restringido del término.

IX. A pesar de que, de acuerdo con la regulación actual de la LECrim y con la establecida en el Anteproyecto de LECrim de 2020, resulta posible obligar a una multinacional tecnológica a la creación de una puerta trasera, la enorme relevancia de esta forma de investigación, que solo irá en aumento, aconseja una regulación expresa de este deber de asistencia.

8. BIBLIOGRAFÍA CITADA

Álvarez Sánchez de Movellán, P.: «Las nuevas medidas de investigación tecnológica y la enésima invocación al principio de proporcionalidad», *Justicia: Revista de Derecho procesal*, 2018, n. 1.

Bachmaier Winter, L.: «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *Boletín del Ministerio de Justicia*, año LXXI, núm. 2195, enero 2017.

Bermúdez González, J. A.: «Deber de colaboración de particulares en la Ley de Enjuiciamiento Criminal», Ponencia presentada en el Curso de formación de Fiscales «Uso de las nuevas tecnologías y nuevas formas de delincuencia», celebrada en el Centro de Estudios Jurídicos los días 27 y 28 de octubre de 2016, disponible en www.cej-mjusticia.es.

Blanco, H.: «El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre», *InDret* 1. 2021.

Escudero García-Calderón, B.: «El investigado o encausado, el abogado y el pariente como sujetos excepcionados del deber de colaborar en la obtención de la prueba digital», *Revista General de Derecho Penal*, núm. 36, 2021.

Gil Gil, A. y Hernández Berlinches, R. (coords.): *Cibercriminalidad*, Dykinson, Madrid, 2019.

González-Cuéllar Serrano, N.: «El principio de proporcionalidad en el Derecho penal español», *Cuadernos de Derecho público*, núm. 5, 1998.

Marchena Gómez, M.: «Algunos aspectos procesales de Internet», en Martín Casallo López, J. J., *Problemática jurídica en torno al fenómeno Internet,* Cuadernos de Derecho Judicial, Escuela Judicial, Consejo General del Poder Judicial, 2000.

— «El sabotaje informático: entre los delitos de daños y desórdenes públicos», *Actualidad informática Aranzadi: revista de informática para juristas*, núm. 40, 2001.

— «Dimensión jurídico-penal del correo electrónico», *Estudios jurídicos*, núm. 2007.

Marchena Gómez, M., y González-Cuéllar Serrano, N.: *La Reforma de la Ley de Enjuiciamiento Criminal de 2015*, Ediciones Jurídicas Castillo de Luna, Madrid, 2015.

Martínez Atienza: *Investigación tecnológica en los ciberdelitos*, Ediciones Experiencia, 2021.

Montes Álvaro, M. A.: «La regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el artículo 18 CE», *Revista del Ministerio Fiscal*, núm. 3, 2017.

Navarro Frías, I.: «El principio de proporcionalidad en sentido estricto: principio de proporcionalidad entre el delito y la pena o balance global de costes y beneficios», *Indret* 2/2010.

Ortiz Pradillo, J. C.:

— «Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica», en Pérez Gil, J. (coord.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar y probar el delito*, La Ley, Madrid, 2012.

— *Problemas procesales de la ciberdelincuencia*, Colex, Madrid, 2013.

Poveda Criado, M. A.: *Delitos en la Red,* Fragua, Madrid, 2015.

Richard González, M.: «La investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal*, núm. 43, septiembre 2017.

Rodríguez Lainz, J. L: «¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?», *Diario La Ley,* núm. 8729, 2016.

— «Veintiocho discrepancias y refutaciones a las Circulares de la Fiscalía General del Estado de 6 de marzo de 2019 sobre diligencias de investigación tecnológica», *Diario La Ley*, núm. 9416, Sección Doctrina, 16 de mayo de 2019.

— «Tres cuestiones polémicas sobre el registro de dispositivos electrónicos de almacenamiento masivo de información», Artículo monográfico, *Revista Sepín*, septiembre 2016.

Rubio Alamillo, J.: «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *Diario La Ley*, núm. 8662, 2015.

Sain, G. y Azzolin, H.: *Delitos informáticos, Investigación criminal, marco legal y peritaje*, IBdef, Montevideo-Buenos Aires, 2017.

Sánchez Melgar, J., *et al.*: Encuesta Jurídica publicada por Sepín en octubre de 2016, disponible en https://sepin.es/cronus4plus/documento/VerDoc.asp?dist=55&referencia=SP%2FDOCT%2F21122&cod=0JP2JP1Cv0FF1T10Vb0FP1%24v0GC0Fa1yB0G909P17P0Vf08A1ek1S308A1vd1yi05u1dF1Dk0Ha1%3DP01b0Fa17T1DT0Fk1C50Gz0Fa1Aa01f0Ha1Aa1Dg0Fa1C42AA0G%5F1C51Cv0FF0yg0HL0GB0Oq01E#25605745

Velasco San Martín, C.: *Jurisdicción y competencia en relación al acceso transfronterizo en materia de ciberdelitos*, Tirant lo Blanch, Valencia, 2016.

Zaragoza Tejada, J. I.: «El registro de dispositivos de almacenamiento masivo de la información», en la obra colectiva dirigida por él, *Investigación tecnológica y derechos fundamentales, Comentarios a las modificaciones introducidas por la Ley 13/2015*, Thomson Reuters Aranzadi, Pamplona, 2017.