Revista Electrónica de Ciencia Penal y Criminología
ISSN 1695-0194

Lo que pasa en tu iPhone, se queda en tu iPhone. A propósito de la desobediencia de las multinacionales tecnológicas

Beatriz Escudero García-Calderón
CUNEF Universidad

ESCUDERO GARCÍA-CALDERÓN, BEATRIZ. Lo que pasa en tu iPhone, se queda en tu iPhone. A propósito de la desobediencia de las multinacionales tecnológicas. *Revista Electrónica de Ciencia Penal y Criminología*. 2022, núm. 24-26, pp. 1-39.
http://criminet.ugr.es/recpc/24/recpc24-26.pdf

RESUMEN: En este artículo se analiza la regulación otorgada por los Ordenamientos francés, alemán, italiano y español al incumplimiento del deber de colaborar en la investigación tecnológica. Se exponen las posibles formas de afrontar este incumplimiento, para llegar a la conclusión de que, si se pretende el castigo de las multinacionales tecnológicas, cuya colaboración en este ámbito resulta decisiva, la respuesta adecuada no está en el delito de desobediencia, sino en la sanciones realistas y eficaces del Derecho administrativo sancionador.

PALABRAS CLAVE: delito de desobediencia; investigación tecnológica; personas jurídicas; pena de multa; sanción administrativa.

TITLE: **What happens on your iPhone, stays on your iPhone. On the disobedience of multinational technology companies**

ABSTRACT: This article intends to analyse the French, German, Italian and Spanish regulations on the breach of the duty to collaborate in technological research. The memo sets out the various ways of facing the referred breach, the conclusion being that if the intention is to sanction the technological multinational companies, the cooperation of which is of utmost importance, the right approach would not be the disobedience offences but the realistic and efficient Public Law sanctions.

KEYWORDS: disobedience offence; technological research; legal entities; criminal fine; administrative penalty.

Fecha de recepción: 15 mayo 2022

Fecha de publicación en RECPC: 31 agosto 2022

Contacto: beatrizescudero@cunef.edu

SUMARIO: 1. La negativa de las empresas tecnológicas a colaborar en la investigación criminal. 2. El incumplimiento de los deberes de colaboración en el derecho comparado: A) Introducción: El Convenio de Budapest. B) Francia. B.1. El delito de negativa a proporcionar el código de descifrado de un medio criptológico. B.2 La agravante de utilización de un medio de cifrado para cometer un delito. C) Alemania. D) Italia. E) España. 3. El delito de desobediencia como respuesta. A) La ineficacia de una pena que no intimida. B) La imposibilidad de castigar a personas jurídicas por un delito de desobediencia. 4. Posibles soluciones de lege ferenda *ante el incumplimiento de las multinacionales tecnológicas. A) Un abordaje penal: la desobediencia genérica o específica como delito susceptible de ser cometido por personas jurídicas. B) Argumentos en contra de una respuesta penal y a favor de la sanción administrativa. 5. Conclusiones. Bibliografía citada.*

---

1. La negativa de las empresas tecnológicas a colaborar en la investigación criminal

A pesar de que recientemente la multinacional tecnológica Apple ha anunciado[1] su polémica intención[2] de colaborar en la lucha contra la pedofilia mediante la instalación de sistemas de vigilancia en sus dispositivos[3], lo cierto es que, desde sus inicios, la compañía estadounidense se ha caracterizado, muy al contrario, por haber desarrollado un modelo de negocio reacio a cualquier actividad que suponga una mínima injerencia en la intimidad de sus clientes. En efecto, con el único objetivo de defender sus propios intereses económicos y diferenciarse de su competidor Google, la empresa de Cupertino ha hecho gala de mantener una política de privacidad[4] sin

[1] La noticia fue adelantada el 5 de agosto de 2021 por el *Financial Times*: https://www.ft.com/content/14440f81-d405-452f-97e2-a81458f5411f, aunque parece que ha quedado en suspenso: https://elpais.com/tecnologia/2021-09-03/apple-retrasa-su-decision-de-escanear-iphones-e-ipads-para-detectar-contenido-pedofilo.html, última consulta: 7-5-2021.

[2] Una idea de lo discutible de esta medida la proporciona el hecho de que para seguir permitiendo que se lleve a cabo este tipo de supervisión, la UE ha tenido que derogar parte de su propia normativa. Así, el Reglamento (UE) 2021/1232 del Parlamento Europeo y del Consejo de 14 de julio de 2021 ha suspendido temporalmente determinadas disposiciones de la Directiva 2002/58/CE. Esta Directiva, conocida como *ePrivacy*, está dedicada a la regulación de la privacidad *online* y de las comunicaciones electrónicas. El nuevo Reglamento permite un control de los servicios de mensajería semejante al que ya estaba siendo realizado por empresas como Google o Microsoft, con el objeto de avisar a las autoridades de cada país de las actividades sospechosas de pedofilia. La colaboración de Google y Microsoft se ha prestado de manera voluntaria, y el hecho de que Apple haya manifestado su disposición de cooperar en este ámbito solamente constituye un reflejo más de esa *curiosa* sensibilidad de la sociedad norteamericana hacia todo lo que tiene un contenido sexual. En todo caso, y como era de esperar, el anuncio de Apple provocó la inmediata respuesta de los sectores sociales defensores de la privacidad, y ello ha llevado a Apple a posponer la implantación del control anunciado.

[3] En concreto, Apple pretende realizar este control en los dispositivos iOS 15, iPadOS15, WatchOS 8 y MacOS Monterey a través de una herramienta de *Machine Learning* denominada *neuralMatch*. Una explicación de las medidas para protección de los niños en https://www.apple.com/child-safety/, última consulta: 20-2-2022.

[4] La última manifestación de esa política la constituye la "App Tracking Transparency", una medida incluida en el iOS 14.5, que permite a los usuarios decidir si permiten o no a las aplicaciones recopilar sus datos con fines publicitarios. Ello ha supuesto unas pérdidas a Facebook, Snapchat, Twitter y YouTube de alrededor

fisuras y, enarbolando la bandera de la protección de datos, se ha autoproclamado custodia de la información de los ciudadanos, negándose, incluso, a colaborar con toda investigación criminal que implique una excepción a su mantra y haciéndolo, además, todo lo abiertamente que le ha resultado posible. Baste recordar a este respecto, la colocación por parte de Apple, con gran olfato empresarial, de una valla publicitaria de enormes dimensiones en el lateral del hotel Marriott de Las Vegas durante la Convención tecnológica CES de 2019, en la que se parafraseaba de manera provocadora el conocido lema de la ciudad del juego: "lo que pasa en tu iphone, se queda en tu iphone".

Semejante eslogan fue utilizado en clara referencia a los enfrentamientos que, con gran repercusión mediática, han protagonizado en los últimos tiempos la todopoderosa multinacional y el Gobierno de los Estados Unidos en el debate relativo al acceso de los investigadores a los teléfonos móviles encriptados[5]. El más conocido tuvo lugar en el año 2016, cuando el FBI trató de que Apple cooperara en el desbloqueo del iPhone de uno de los autores de la masacre de San Bernardino. En el tiroteo llevado a cabo en diciembre de 2015, resultaron abatidos los propios autores de la matanza, Malak y Syed Farook. Con el objetivo de determinar si los terroristas habían actuado solos o pertenecían a una cédula yihadista, el FBI intentó registrar el contenido del iPhone 5 hallado entre las pertenencias de Syed. No obstante, el FBI no logró desbloquear el dispositivo porque, a pesar de disponer del cadáver de Farook y, por tanto, de su huella digital, al tratarse de un modelo antiguo, solamente era posible el acceso mediante la introducción de la contraseña numérica[6]. Por este motivo, acabaron solicitando la cooperación de la empresa fabricante, Apple Inc. Obtuvieron incluso la orden judicial pertinente. Apple, sin embargo, se negaría a colaborar aduciendo el peligro que suponía la creación de una puerta trasera (*backdoor)*, y así lo hizo saber públicamente el Presidente de la empresa de la manzana, Tim Cook, mediante una carta abierta a sus clientes[7]. El FBI finalmente optó por

de 10.000 millones de dólares. Como es por todos conocido, Facebook ha llevado esa confrontación a la publicidad de los periódicos nacionales. A pesar de que Apple ha intentado vestir nuevamente su maniobra en el mercado de la publicidad online con su tradicional disfraz buenista de la protección de datos, lo cierto es que, como bien apuntaba el *Wall Street Journal*, Apple busca su parte de un mercado dominado por Google y Facebook. Véase: https://www.macworld.com/article/344420/app-tracking-transparency-privacy-ad-tracking-iphone-ipad-how-to-change-settings.html y el artículo del Wall Street Journal, "Apple's Privacy Changes Are Poised to Boost Its Ad Products", en https://www.wsj.com/articles/apples-privacy-changes-are-poised-to-boost-its-ad-products-11619485863?mod=mh, últimas consultas: 1-3.2022.

[5] Puede leerse un análisis en profundidad del conflicto en RODRÍGUEZ LAINZ, 2016, pp. 1-6.

[6] Realmente, hubo un error previo por parte del FBI. Por error, restablecieron de forma remota la contraseña de la cuenta de *iCloud* de Apple asociada con el dispositivo, lo que impidió que se realizara una copia automática en *iCloud*. La equivocación fue reconocida por el propio FBI en un comunicado en el que alegaron que igualmente hubieran requerido la cooperación de Apple para acceder a la totalidad de la información contenida en el móvil y que no se almacena en la nube en ningún caso. Véase: https://abcnews.go.com/US/fbi-chief-admits-mistake-iphone-wake-san-bernardino/story?id=37314654, última consulta: 3-1-2022.

[7] La respuesta de Tim Cook en forma de carta a sus clientes está disponible en https://www.apple.com/customer-letter/, última consulta: 3-1-2022.

recurrir a la empresa israelí *Cellebrite*[8], y solamente tras cuatro meses de espera y previo pago de 900.000 dólares, pudo acceder a la información contenida en el iPhone de Farook.

A partir de entonces, la negativa de Apple a colaborar se convertiría en una constante. El mismo año del tiroteo de San Bernardino, el FBI requirió la colaboración de la empresa de la manzana para acceder al móvil de un narcotraficante, y ante la negativa de la multinacional a cooperar, el FBI solicitó una orden judicial que le sería finalmente denegada por un Juez de Brooklyn. Posteriormente, en 2019, el FBI pretendió de nuevo la ayuda de Apple, con el objeto, esta vez, de desbloquear dos móviles pertenecientes a un supuesto terrorista que había participado en el atentado perpetrado en una Base naval de Florida. Como era de esperar, también en este supuesto Apple rechazó desbloquear el terminal telefónico, y ello derivó en un enfrentamiento sin precedentes entre el Gobierno de los EEUU y la multinacional norteamericana que, hoy por hoy, sigue sin encontrar solución, y en el que ha tomado partido incluso la Oficina de Derechos Humanos de la ONU[9].

La pertinaz negativa de Apple a colaborar ha llevado a los investigadores de distintos países a buscar soluciones alternativas para garantizarse el acceso a los dispositivos cifrados. A la misma empresa *Cellebrite* utilizada por el FBI recurrió en nuestro país la UCO para tratar de acceder a la información contenida en el teléfono móvil de la tristemente desaparecida Diana Quer[10]. Su iPhone 6 había sido encontrado por un mariscador en las inmediaciones de muelle de Taragoña en mal estado tras pasar dos meses sumergido en agua. Los datos del móvil de José Enrique Abuín, alias "el Chicle", no pudieron ser utilizados,[11] pero la triangulación del móvil de Diana, de las señales telefónicas y del GPS, además del contenido de sus mensajes, resultaron cruciales para desmontar la defensa de "el Chicle", que nunca estuvo con ella donde él afirmaba. A la opinión pública trascendió únicamente el dato de que los servicios de *Cellebrite* habían costado unos llamativamente escasos 2.000 euros. No obstante, conviene poner nuevamente de manifiesto el retraso forzoso que implica acudir a estas vías alternativas: la empresa israelí entregó su informe en julio de 2017, cuando las diligencias del caso estaban archivadas desde abril de ese año. En el caso de Diana

[8] Existe una versión alternativa, publicada por *The Washington Post* el 12 de abril de 2016 (https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html, última consulta: 14-1-2022), de acuerdo con la cual el FBI no habría recurrido a *Cellebrite,* sino a los servicios de unos *hackers* mercenarios de *Azimuth*, una empresa dedicada a buscar fallos de seguridad en los sistemas de gobiernos autoritarios.

[9] Puede verse el contenido de la declaración del Alto Comisionado de la ONU para los Derechos Humanos, favorable a la postura de Apple, en https://www.nytimes.com/2016/03/05/technology/un-apple-gunman-iphone.html, última consulta: 11-1-2022.

[10] Véase, por ejemplo, https://www.elmundo.es/sociedad/2017/07/06/595e193f22601d5a068b45ce.html y https://elpais.com/politica/2017/07/06/actualidad/1499325032_475830.html, última consulta: 14-1-2022.

[11] Abuín formateó su teléfono haciendo desaparecer los datos. Su ubicación no había sido detectada por ninguna antena de telefonía. Véase: https://www.elcorreogallego.es/hemeroteca/chicle-entrego-guardia-civil-movil-formateado-horas-antes-comenzo-actuar-sigilo-CRCG1213980, última consulta: 20-1-2022.

Quer, sin embargo, no consta que existiera una orden judicial exigiendo la colaboración de Apple, ni que ésta se hubiera solicitado de algún modo, a pesar de que en España este enfrentamiento entre la justicia y los empresas tecnológicas -o lo que es lo mismo, entre el Estado y el sector privado- había sido, al menos en apariencia, zanjado en tiempos recientes con la reforma de la Ley de Enjuiciamiento Criminal. En efecto, mediante la Ley Orgánica 13/2015, de 5 de octubre[12], el legislador de las nuevas tecnologías, con el objetivo de que los encargados de investigar delitos pudieran tener acceso a una información relevante desde el punto de vista penal que, de otro modo, les resultaría inalcanzable, se posicionó claramente del lado del Estado, estableciendo para un círculo muy amplio de sujetos del sector privado una serie de deberes de colaboración que han sido mantenidos con parecida regulación en el Anteproyecto de Ley de Enjuiciamiento Criminal[13]. De esta manera, todo aquel que sepa cómo acceder a unos datos relevantes para una investigación que se hallen contenidos en un dispositivo electrónico[14] queda obligado a contribuir a la causa de la justicia, ya sea manejando el *software*, revelando cómo eludir medidas de seguridad o de autenticación, desvelando claves de acceso o comunicando la ubicación de datos concretos.

A reflexionar acerca de cómo se castiga el incumplimiento de los deberes de colaboración que pesan sobre el sector privado, nos gustaría dedicar estas líneas, no sin poner previamente de manifiesto que la elección de multinacional Apple para ejemplificar el enfrentamiento entre el sector público y el privado y, de paso, dar título a esta contribución, se debe a la enorme popularidad de la compañía norteamericana. No obstante, el conflicto no se circunscribe a la empresa de la manzana. Recordemos, por ejemplo, que en 2021 la prensa española se hizo eco de las dificultades de la

[12] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim para el reforzamiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE N° 239, de 6.10.2015).

[13] Los deberes de colaboración en el registro de dispositivos de almacenamiento masivo pasan del art. 588 sexies c.5 al 428, con la misma referencia a la carga desproporcionada como límite objetivo y con el mismo apercibimiento para quien no colabore de incurrir en delito de desobediencia. Se reforma el límite subjetivo, que pasa a añadir como sujetos excepcionados del deber de colaborar a la persona investigada o encausada, al pariente y a "aquellas que no pueden declarar en virtud del secreto profesional". El deber de colaboración en los registros remotos pasa del art. 588 septies b.) LECrim al 432 en el Anteproyecto. La redacción es la misma (salvo en el mismo añadido en cuanto al límite subjetivo). Por lo tanto, todo lo que aquí se afirma, rige también para la nueva LECrim.

[14] Empleamos el calificativo de "electrónico" por su aceptación en el lenguaje común y en el debate jurídico, siendo conscientes de su incorrección. Como señala RUBIO ALAMILLO, 2015, pp. 2 y 3, lo apropiado es utilizar el calificativo de "informático", pues la informática se encuentra en un orden de abstracción mayor y hace referencia a los dispositivos en que se ejecutan programas y que requieren obligatoriamente la interacción del usuario, frente a un simple dispositivo electrónico, como puede ser una nevera o un televisor. En el ámbito del Derecho, sin embargo, la calificación de "electrónica" es usual, como lo demuestran las más de cien entradas del término en Dialnet.

Policía Científica para acceder al contenido de la tarjeta de memoria de Dina Bousselham[15]. Tras haberse requerido sin éxito, hasta en dos ocasiones, a la empresa Samsung una serie de datos técnicos –los relativos al *pinout* del interfaz NAND de la tarjeta MicroSD- necesarios para llevar a cabo el análisis de la tarjeta del teléfono móvil de la ex-asesora de Pablo Iglesias, llegó incluso a encargarse a una empresa británica valorar la posibilidad de recuperar la información de la micro tarjeta SD. Finalmente, el juez Manuel García Castellón, tras advertir "de modo expreso a la entidad receptora, en la persona del Director de Departamento de Asesoría jurídica de Samsung Electronics Iberia", de que su negativa podía dar lugar a un delito de desobediencia[16], ordenó la colaboración de la empresa coreana, obligándola a suministrar "los pines tecnológicos de la memoria" así como "la información relativa a las transformaciones que realice la controladora de la tarjeta durante el proceso de lectura y escritura de la información" para poder, no solo llevar a cabo la lectura de la tarjeta, sino también interpretar los datos contenidos en la misma. Samsung se avino a colaborar en el último momento[17] e incluso llegó a informar de la viabilidad de esa recuperación por medio de un *software* específico, pero por razones ajenas a Samsung, finalmente el programa informático no llegó a utilizarse y el caso se cerraría tras unas declaraciones de la propia Dina Bousselham sin llegar a hacerse efectiva la cooperación de la empresa coreana.

Los tres casos mencionados -San Bernardino, Diana Quer y Dina Bousselham- ponen de manifiesto que ya en la actualidad, de manera generalizada, el éxito en la investigación criminal, -y no digamos en el ámbito de la ciberdelincuencia-, pasa irremediablemente por la cooperación, devenida imprescindible, del sector privado. Lógicamente, solo existe un deber -en este caso de colaborar- en la medida en que una sanción jurídica castiga su incumplimiento. Precisamente de la sanción que se aplica a esas multinacionales tecnológicas en caso de negarse a cooperar, nos ocuparemos en esta contribución.

2. **El incumplimiento de los deberes de colaboración en el derecho comparado**

A) ***Introducción: El Convenio de Budapest***

A pesar de que la dependencia del investigador criminal respecto de la colaboración del sector privado ha crecido de manera exponencial en los últimos años, lo

[15] Por todas, https://www.abc.es/espana/abci-samsung-entregara-directamente-policia-claves-para-destripar-tarjeta-dina-bousselham-202110081401_noticia.html, última consulta: 10-3-22.

[16] Véase: https://www.abc.es/espana/abci-juez-requiere-samsung-para-informe-sobre-tarjeta-dina-bajo-pena-desobediencia-202109151039_noticia.html, última consulta: 12-3-22.

[17] Véase: https://www.abc.es/espana/abci-samsung-entregara-directamente-policia-claves-para-destripar-tarjeta-dina-bousselham-202110081401_noticia.html, última consulta: 10-3-22.

cierto es que esa relación de subordinación y de necesidad fue intuida ya por el importante Convenio de Budapest sobre ciberdelincuencia, de 23 de noviembre de 2001, ratificado por España en 2010. Prueba de ello es que en su art. 19.4 se exhortaba a los Estados parte a que adoptaran "las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a 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 toda la información necesaria, dentro de lo razonable (…)"[18].

El llamado Ciberconvenio constituye, como es sabido, el primer Tratado internacional sobre delitos cometidos a través de sistemas informáticos. Se centraría, fundamentalmente, en la armonización de las legislaciones penales y procesales, en el establecimiento de un régimen de cooperación entre Estados ágil y eficaz, y en la mejora de las técnicas de investigación de los Estados firmantes.[19] Puede considerarse, en este sentido, como el precursor en Europa de todas las leyes que vendrían después a tratar de eliminar, o al menos de disminuir, el blindaje proporcionado a los delincuentes gracias a la confidencialidad característica de las nuevas tecnologías. Así pues, desde su adopción, los distintos Estados han establecido deberes de colaboración de mayor o menor amplitud sobre el sector privado, aunque la fórmula por la que se ha optado ha variado de un Estado a otro.

A pesar de los enormes cambios experimentados desde el año 2001 en el mundo de las nuevas tecnologías, conviene recordar que ese deber de colaboración, previsto ya de manera premonitoria, como decimos, en el Ciberconvenio, se ha erigido en uno de los pilares de la investigación criminal. No se puede perder de vista que, desde el inicio mismo de la revolución tecnológica, existe una clara confrontación entre el sector público y el privado por los distintos intereses que inspiran a uno y otro: el investigador criminal quiere acceder al dispositivo electrónico para encontrar pruebas y la multinacional vende productos valiosos precisamente por su inaccesibilidad. Esa dificultad para acceder a los dispositivos electrónicos, presente, como decimos, desde los inicios, ha crecido en los últimos años de manera vertiginosa, llegando a alcanzarse un blindaje total gracias a las innovaciones técnicas. Un hito en este ámbito lo constituye el sistema operativo iOS 8, con el que Apple introdujo en sus productos unos sistemas de retardo en el acceso y de autodestrucción de datos que supusieron un antes y un después para la investigación criminal. El primero sistema lograba que, tras la introducción de cuatro contraseñas erróneas, hubiera que esperar un tiempo antes de volver a probar un nuevo código. Ese tiempo aumentaba exponencialmente tras cada intento. El sistema de autodestrucción, por su parte, supuso

[18] Lo que no puede considerarse razonable se ha trasladado a la LECrim con el término "carga desproporcionada" en el ámbito del registro directo de dispositivos de almacenamiento masivo de datos. Al análisis de este concepto y del de "facilitación de información", dedico el artículo, todavía en prensa, que aparece en la bibliografía.

[19] Véase una información detallada en LÓPEZ BARJA DE QUIROGA, 2014, pp. 2012 y ss.

la posibilidad de seleccionar la eliminación automática de todos los datos contenidos en el dispositivo tras la introducción de 10 contraseñas erróneas. Y aunque estos sistemas fueron patentados por la empresa de la manzana, lo cierto es que todas las empresas relacionadas con las nuevas tecnologías han conseguido tremendos avances: baste traer a la memoria el llamado cifrado "de extremo a extremo"[20] que utiliza cualquier aplicación que permite la comunicación escrita, como *WhatsApp*. Semejantes avances tecnológicos han provocado que esa dependencia en otro tiempo *controlada* del sector público respecto del privado se haya convertido en absoluta. De ahí que los legisladores de los distintos países hayan reforzado en sus respectivos Ordenamientos los deberes de colaboración sobre el sector privado. En todo caso, cada Estado ha optado por un abordaje distinto de esta problemática, lo que ha llevado también a su sanción por medio de diferentes mecanismos. Pasamos a exponer las opciones legislativas por las que han optado en el Derecho comparado Francia, Alemania e Italia, para acabar con una referencia a la fórmula elegida por el legislador español.

B) ***Francia***

De entre todos los Estados europeos firmantes del Convenio de Budapest, el país que con mayor severidad y contundencia ha reaccionado frente a la confidencialidad y el anonimato que aportan las nuevas tecnologías es, probablemente, Francia. Así, desde el año 2001 se ha tipificado como delito de omisión pura la mera negativa a proporcionar las claves para acceder a un dispositivo, y desde el 2004 se ha incluido como agravante la comisión de un delito a través de un dispositivo electrónico. Veamos ambas normas.

B.1. *El delito de negativa a proporcionar el código de descifrado de un medio criptológico*

En la Sección 2 del Código penal francés, dedicada a la obstrucción a la justicia[21] dentro del Capítulo IV, bajo la rúbrica "Atentados a la acción de la justicia", la Ley n. 2001-1062, de 15 noviembre ha incorporado un nuevo delito de omisión pura. De acuerdo con ello, actualmente el art. 434-15-2 CP castiga con tres años de prisión y multa de 270.000 euros a "todo aquel que, teniendo conocimiento de la convención secreta de descifrado de un medio criptológico susceptible de haber sido utilizado para preparar, facilitar o cometer un delito o una infracción, se negare a proporcionarlo a las autoridades judiciales o ejecutarlo, en los requerimientos de estas autoridades dictados de conformidad con los Títulos II y III del Libro I del Código Procesal

[20] En este tipo de cifrado, el mensaje viaja encriptado, de forma que solamente puede ser descifrado por el dispositivo destinatario del mensaje. En el llamado "cifrado de datos en tránsito", por el contrario, los mensajes se descifran en el servidor, se vuelven a cifrar, se envían, y son descifrados nuevamente por el receptor.

[21] "Des entraves à l'exercice de la justice".

Penal". Y se añade en un segundo párrafo que "cuando la entrega o la ejecución del código hubiera permitido evitar la comisión de un delito o una infracción o limitar sus efectos, la pena se eleva a cinco años de prisión y a 450.000 euros de multa"[22].

Por lo tanto, se castiga cumulativamente, con una pena de prisión y multa, –cuya cuantía ha aumentado, por cierto, significativamente, tras la reforma de 2016[23]- a *todo aquel* que se niegue a proporcionar la "convención secreta de descifrado de un medio criptológico", siempre que se den dos circunstancias: que existan indicios de que el medio haya sido utilizado para preparar, facilitar o cometer un delito y que el código de acceso haya sido solicitado por la autoridad judicial. Se añade un subtipo agravado en el apartado segundo, que castiga con mayor severidad esa misma omisión si la colaboración, de haberse prestado, hubiera impedido la comisión de un delito o paliado sus efectos.

Conviene, por tanto, primero, definir qué se entiende por "convención secreta". Con esta expresión se designa en ciberseguridad una clave mantenida fuera del conocimiento de terceros y utilizada en un servicio de cifrado[24]. El cifrado consiste en la conversión de datos a un formato secreto que asegura su confidencialidad. Esos datos se alteran para que parezcan aleatorios, utilizando una clave que permite cifrarlos y descifrarlos, convirtiéndolos, respectivamente, en ilegibles y en legibles según convenga. El cifrado constituye la base de la seguridad de datos. Se trata de la forma más sencilla e importante de garantizar que la información de un sistema informático, de muy diversa naturaleza[25], no pueda ser leída o procesada por terceros. Por ello su uso se ha generalizado a nivel mundial para proteger la información de los usuarios. Para lograr esa protección, se utiliza un *software* de cifrado de datos, también conocido como "algoritmo de cifrado", que permite desarrollar lo que se conoce como un "esquema de cifrado". Ese esquema, al menos en teoría, solo puede deshacerse mediante el uso de una enorme potencia informática. Por lo tanto, el algoritmo necesario para descifrar los datos es la "convención secreta" cuya ejecución o facilitación a las autoridades exige el legislador en el Código penal francés.

El cifrado fue regulado en Francia por el Decreto n. 98-102, de 24 de febrero de 1998, por el que se definen las condiciones en las que se aprueban las organizaciones

[22] Article 434-15-2 CP: "Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.Si le refus est opposé alors que la remise ou la mise en oeuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende".

[23] Nos referimos a la reforma operada por Ley n. 2016-731, de 3 junio de 2016, de refuerzo contra el crimen organizado, el terrorismo, su financiación y mejora de la eficacia y de las garantías del proceso penal. Las cuantías aumentaron significativamente pues, con anterioridad a la reforma, las penas de multa eran de 45.000 euros para el tipo básico y de 75.000 euros para el tipo agravado, respectivamente.

[24] https://www.answeb.net/fr/glossaire-internet/id-100-convention-secrete, última consulta: 10-3-22.

[25] Incluyendo desde información personal hasta pagos, por ejemplo.

que gestionan las convenciones secretas de criptología en nombre de otros, de conformidad con el artículo 28 de la Ley n. 90-1170, de 29 de diciembre de 1990, sobre la regulación de las telecomunicaciones. En el art. 1.1 del Decreto se definía la convención secreta como las claves inéditas necesarias para la implementación de un medio o servicio criptológico destinado a operaciones de cifrado o descifrado[26]. Finalmente, la Ley n. 2004-575, de 21 de junio, de confianza en la economía digital[27] ha incluido una definición de la "convención secreta de un medio de criptología", estableciendo en su art. 29 que "por medio de criptología se entiende cualquier *hardware* o *software* diseñado o modificado para transformar datos, ya sean informaciones o señales, utilizando convenciones secretas o para realizar la operación contraria con o sin convención secreta. Estos medios criptográficos están destinados principalmente a garantizar la seguridad del almacenamiento o transmisión de datos, al permitir asegurar su confidencialidad, su autenticación o el control de su integridad"[28].

A pesar de esta definición legal, lo que ha de entenderse por "convención secreta de descifrado de un medio criptológico" no constituye una cuestión pacífica[29]. En principio, una convención capaz de cifrar o descifrar lo constituye todo *hardware* o *software* dedicado al cifrado. De esta manera, podría pedirse la cooperación de las multinacionales tecnológicas al amparo de este precepto. Más problemática resulta, sin embargo, la cuestión de si puede calificarse de convención secreta el código de acceso a un teléfono móvil. En la interpretación de este concepto, generadora de una enorme polémica en Francia[30], resulta de gran interés la Sentencia de la Corte de Casación francesa de 13 de octubre de 2020: un hombre, tras haber sido detenido por su participación en varios delitos flagrantes relacionados con el tráfico de drogas, fue requerido por la policía durante el interrogatorio para que comunicara los códigos de desbloqueo de los tres teléfonos móviles que se encontraban en su poder y, al negarse, el Juzgado de lo Penal competente lo condenó, además de por diversos delitos relacionados con el tráfico de drogas, por la negativa a presentar una convención de descifrado de un medio criptológico, previsto en el artículo 434-15-2 del Código penal francés.

[26] Art. 1. 1° "Conventions secrètes: des clés non publiées nécessaires à la mise en oeuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement".

[27] *Loi 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique.* En francés, el término "digital" se reserva estrictamente para lo relativo a los dedos, mientras que al hacer referencia a lo que nosotros denominamos "medios digitales" se emplea el calificativo de "numérico".

[28] Art. 29: "On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité".

[29] Véase al respecto UDIBERT, 2020, pp. 24 y ss., disponible en https://hal.archives-ouvertes.fr/hal-02991975/document, última consulta 26-2-22 y BONIS/ PELTIER, 2018, pp. 72 y ss.

[30] Véanse, por ejemplo, ROUSSEL, 2020, pp. 146 y ss., DE COMBLES DE NAYVES, 2019, pp. 439 y ss. y DERIEUX, 2018, pp. 1 y ss.

El individuo recurrió y el Tribunal de Apelación de París (*Cour d'appel de Paris*) en la Sentencia n. 18/09267, de 16 de abril de 2019, lo absolvió con dos argumentos: el de que la solicitud realizada por un oficial de policía no constituye el "requerimiento por parte de una autoridad judicial" que exige el tipo[31], y el de que un código de desbloqueo de un teléfono móvil de "uso común" no constituye propiamente una "convención secreta de un medio criptológico", puesto que no permite el descifrado de datos o mensajes, sino que simplemente permite el acceso, en el sentido de que lo abre, a los datos contenidos en ellos.

En la determinación de estos conceptos, puede decirse que una tercera fase se inicia cuando el Fiscal General de la Corte de Casación recurre en casación "en el único interés de la ley". En la Sentencia n. 20-80.150, de 13 de octubre de 2020, la Corte de Casación rechazará la fundamentación de la sentencia del Tribunal de Apelación. Así, en primer lugar, consideró que el requisito del tipo relativo a la existencia de requerimientos dictados por la autoridad judicial se da cuando el requerimiento es dictado por un agente de policía judicial que actúe al amparo de los artículos 60-1, 77-1-1 y 99-3 del Código procesal penal francés (*Code de procédure pénale*), bajo el control de la autoridad judicial. Por lo tanto, se admite que, en el marco de una investigación de un delito flagrante, como era el caso, los requerimientos puedan provenir de la policía judicial. No obstante, considera la Corte que la petición por parte de los policías había consistido en una simple solicitud realizada durante una audiencia, sin advertir de que la negativa a cumplir podía ser constitutiva de delito, por lo que, en sentido estricto, debido a este déficit, no se estaba ante un verdadero requerimiento. De esta manera, aunque teóricamente pudiera considerarse en determinadas circunstancias el requerimiento de la policía judicial como un requerimiento dictado por la autoridad judicial, también es necesario que se den en él una serie de requisitos formales que no se reunían en el caso en cuestión.

La Sala de lo Penal de la Corte de Casación, por lo demás, rechazó el argumento de que un código de desbloqueo de un teléfono de "uso común" no pudiera ser calificado como "convención secreta de un medio criptológico," de acuerdo con el art. 434-15-2 del Código penal francés. Para fundamentar su oposición recurrió al art. 29 de la Ley sobre confianza en la economía digital, de 21 de junio de 2004, al que ya hemos hecho referencia, y que define el medio de criptología como cualquier *hardware* o *software* diseñado o modificado para transformar datos, utilizando convenciones secretas, o para realizar la operación contraria con o sin convención secreta. De esta manera, la Corte de Casación consideraría que no todo código no revelado se subsume en este tipo penal: solamente es así cuando el dispositivo dispone de un medio de cifrado. De este modo, viene a afirmar que el código de desbloqueo de un teléfono móvil puede constituir esa convención secreta de la que habla el Código

[31] El Consejo Constitucional se había manifestado ya en contra de asimilar un oficial de policía judicial a la autoridad judicial. Véase, por ejemplo, la sentencia n. 93-326 D, de 11 de agosto de 1993.

penal francés, siempre y cuando el teléfono en cuestión sea uno de los llamados "teléfonos inteligentes" (*smartphones*).

Por lo tanto, en la actualidad, parece que el precepto resulta aplicable a todo aquel que conozca el funcionamiento del *software* de descifrado[32], incluyéndose en ese círculo a quienes conozcan la clave de acceso de un teléfono "inteligente", provisto, como decimos, de ese medio de cifrado que exige la Corte de Casación francesa. Y puesto que el Código penal francés se refiere a "todo aquel" (*quiconque*) y omite la introducción de excepción alguna, resulta aplicable tanto a un tercero que conozca el código de acceso, como al propio titular del dispositivo, a pesar de que fuera él mismo quien resultara investigado o encausado. Es más, lo cierto es que, en la práctica, su aplicación se ha limitado hasta ahora a casos en los que el propio titular de un dispositivo se negaba a proporcionar el código de acceso, lo que ha generado lógicas dudas acerca de la posible incompatibilidad de este delito con unos cuantos principios constitucionales[33]. Finalmente, la cuestión ha sido zanjada por el Consejo Constitucional francés, en la Sentencia n. 2018-696 *QPC* (cuestión prioritaria de constitucionalidad) de 30 de marzo de 2018. El Consejo Constitucional se pronunciaría sobre este asunto a través de ese control *a posteriori* de la constitucionalidad de las leyes francesas, introducido con la reforma constitucional de 2008[34]: se afirmó la conformidad del precepto con la Constitución al considerarse acorde con el debido respeto al derecho al silencio, al derecho a la no autoincriminación, al derecho a la intimidad y al derecho al secreto de las comunicaciones. El Consejo Constitucional subrayó que "el legislador ha perseguido los objetivos de valor constitucional de prevenir los delitos y encontrar a los autores de los delitos, ambos necesarios para salvaguardar derechos y principios de valor constitucional"[35]. Además, se consideró que con una obligación de esta naturaleza ni se busca obtener una confesión, ni se impone con la misma ningún tipo de reconocimiento; y con el argumento de que la investigación o la instrucción tiene que haber permitido identificar la existencia de datos tratados por medios criptológicos susceptibles de haber sido utilizados para preparar, facilitar o cometer un delito o una infracción, se justificó la medida, recha-

[32] Acerca de las lagunas existentes a día de hoy y de la necesidad de un procedimiento que garantice la integridad de las pruebas así obtenidas, véase, por ejemplo, ROUSSEL, 2020, p. 147.

[33] Según consta en el apartado 2 de la Sentencia n° 2018-696 QPC de 30 de marzo de 2018, quienes plantearon su inconstitucionalidad alegaban su incompatibilidad con el derecho al silencio, el derecho a no contribuir a la autoincriminación, el derecho a un proceso justo y equitativo garantizado por el artículo 16 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789 y con la presunción de inocencia garantizada por el artículo 9. Alegaron también la vulneración del derecho al respeto de la vida privada, el secreto de la correspondencia, los derechos de defensa, el principio de proporcionalidad de las sanciones y la libertad de expresión. Texto disponible en: https://www.legifrance.gouv.fr/jorf/id/JORFARTI000036756810#JORFARTI000036756810

[34] Explican con detalle el complejo procedimiento relativo al control *a posteriori* de la constitucionalidad de las leyes (sentencias *QPC*), CERDA GUZMÁN/ GUGLIELMI, 2021, pp. 65-72.

[35] Sentencia n. 2018-696 *QPC* de 30 de marzo de 2018, párrafo 7.

zándose igualmente la posible vulneración del derecho al secreto de las comunicaciones. Por último, el Consejo Constitucional esgrimió el tradicional argumento de la existencia independiente de la prueba respecto de la voluntad del sospechoso[36]: al tratarse de un código ya fijado en un soporte, tiene un carácter autónomo respecto de lo que el investigado quiere y, por lo tanto, no está cubierto por su derecho a la no autoincriminación.

En definitiva, la regulación francesa, y especialmente la interpretación jurisprudencial que de la misma se viene haciendo, han generado un deber de colaboración en la investigación tecnológica muy particular. Para que surja el deber de colaborar basta con conocer la llamada "convención secreta", pudiendo consistir ésta incluso en la contraseña de un teléfono móvil inteligente. Resulta posible exigir esa cooperación por parte de la autoridad judicial a cualquier sujeto, desde un *hacker* a los miembros de una multinacional tecnológica, y el concepto de autoridad judicial ha de ser en sentido amplio. Al no introducir la ley excepción alguna, el deber de colaborar rige incluso para el propio titular del dispositivo, que es a quien en la práctica viene exigiéndose hasta ahora. La colaboración puede consistir, alternativamente, en proporcionar la "convención secreta", o en ejecutarla. Como de acuerdo con el art. 434-15-2 CP, es preciso que el dispositivo haya sido utilizado para "preparar, facilitar o cometer" un delito, quedarán fuera de esta obligación los dispositivos que contengan información relacionada con una actividad delictiva pero que no tengan relación directa con la comisión de un delito. Por lo tanto, quedan afectados por este deber los dispositivos empleados en la comisión de un ciberdelito en sentido estricto, esto es, los delitos cometidos contra un sistema informático (el sabotaje y el hackeo), y los ciberdelitos en sentido amplio, es decir, los delitos cometidos a través de un sistema informático (una estafa, un ciberacoso, por ejemplo)[37]. Pero no sucederá lo mismo con los delitos analógicos, salvo que el dispositivo haya facilitado de algún modo su comisión.

B.2 *La agravante de utilización de un medio de cifrado para cometer un delito*

Además de la sanción por la no facilitación de la convención secreta de descifrado, la utilización de un medio criptológico para preparar o cometer un delito grave (*crime*)[38] o menos grave (*délit*), o para facilitar su preparación o comisión, constituye una circunstancia agravante genérica en Francia desde el año 2004. Así lo establece

[36] La posibilidad de aplicar este argumento a las claves de acceso a un dispositivo electrónico la analicé en 2021, pp. 33 y 34.

[37] La distinción entre ciberdelitos en sentido amplio, como aquellos delitos tradicionales cometidos a través de un sistema informático, y ciberdelitos en sentido estricto, como aquellos cometidos contra un sistema informático, es aceptada de forma generalizada en la doctrina. A este respecto puede verse, por ejemplo, VELASCO NÚÑEZ, 2010, p. 41 y DAVARA FERNÁNDEZ DE MARCOS, E./ DAVARA FERNÁNDEZ DE MARCOS, L., 2017, p. 29 y ss.

[38] El término "crime" está reservado a los delitos castigados con pena de prisión de al menos diez años.

el art. 132-79[39], que despliega, en batería, los correspondientes aumentos de las posibles penas: prisión permanente cuando el delito se castiga con pena de hasta treinta años; treinta, cuando se castiga con prisión de hasta veinte; quince cuando es de prisión hasta diez; diez cuando la pena es de prisión hasta siete; siete cuando la prisión es hasta cuatro y el doble de pena cuando la pena es de prisión hasta tres años. El medio criptológico o de cifrado ha de ser uno de aquellos a los que se refiere el art. 29 de la Ley 2004-575, de 21 de junio, al que ya hemos hecho referencia en el apartado anterior. En todo caso, de acuerdo con el último párrafo del precepto, es posible no aplicar la agravante cuando, a solicitud de las autoridades judiciales o administrativas, el autor o cómplice entreguen la versión descifrada de los mensajes, así como las claves secretas para descifrarlo.

C) *Alemania*

En el año 2021 se aprobó en Alemania la Ley de Regulación de Protección de Datos y Privacidad en Telecomunicaciones y Telemedios, de 23 de junio. Dicha Ley vino a alinear la normativa con el Reglamento europeo de Protección de datos, en vigor desde el 24 de mayo de 2016 y, sobre todo, a regular de manera unificada la protección de datos en dos sectores, el de las Telecomunicaciones y el Audiovisual, hasta entonces escindidos en sendas leyes: la Ley de Telecomunicaciones y la Ley de Servicios de la Sociedad de la Información. De acuerdo con la modificación efectuada por esta Ley de Regulación de Protección de Datos y Privacidad en Telecomunicaciones y Telemedios, el Código de Procedimiento penal alemán (S*trafprozeßordnung*; en sus siglas StPO) establece en el § 100j[40] una serie de deberes de

[39] Este artículo, introducido por Ley 2004-575, de 21 de junio, de confianza en la economía digital, establece: "Lorsqu'un moyen de cryptologie au sens de l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a été utilisé pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue est relevé ainsi qu'il suit :

1° Il est porté à la réclusion criminelle à perpétuité lorsque l'infraction est punie de trente ans de réclusion criminelle;

2° Il est porté à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion criminelle;

3° Il est porté à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion criminelle;

4° Il est porté à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement;

5° Il est porté à dix ans d'emprisonnement lorsque l'infraction est punie de sept ans d'emprisonnement;

6° Il est porté à sept ans d'emprisonnement lorsque l'infraction est punie de cinq ans d'emprisonnement;

7° Il est porté au double lorsque l'infraction est punie de trois ans d'emprisonnement au plus.

Les dispositions du présent article ne sont toutefois pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires ou administratives, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement".

[40] § 100j "Bestandsdatenauskunft

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt warden:

1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172

colaboración sobre quienes participan en las telecomunicaciones y tienen, por ese motivo, obligación de inventariar y conservar determinados datos. De acuerdo con ello, puede solicitarse información a estos sujetos obligados en la medida en que sea necesario para investigar unos hechos o determinar el paradero de una persona acusada de la comisión de un delito. Esta información engloba la relativa a los códigos de seguridad de acceso[41] almacenados por los proveedores, como contraseñas, PIN, y PUK.

El carácter obligatorio de esta cooperación aparece contemplado en el párrafo 5 del § 100j StPO, donde se preceptúa que, ante una solicitud de información, la per-

des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, und

2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Telemedien-Datenschutz-Gesetzes (§ 22 Absatz 1 Satz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes) von demjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.

Bezieht sich das Auskunftsverlangen nach Satz 1 Nummer 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 174 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. 3Bezieht sich das Auskunftsverlangen nach Satz 1 Nummer 2 auf als Bestandsdaten erhobene Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 23 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für ihre Nutzung zur Verfolgung einer besonders schweren Straftat nach § 100b Absatz 2 Nummer 1 Buchstabe a, c, e, f, g, h oder m, Nummer 3 Buchstabe b erste Alternative oder Nummer 5, 6, 9 oder 10 vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3, § 177 Absatz 1 Nummer 3 des Telekommunikationsgesetzes und § 22 Absatz 1 Satz 3 und 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes). Das Vorliegen der Voraussetzungen für ein Auskunftsverlangen nach Satz 1 ist aktenkundig zu machen.

(3) Auskunftsverlangen nach Absatz 1 Satz 2 und 3 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Im Fall von Auskunftsverlangen nach Absatz 1 Satz 2 kann die Anordnung bei Gefahr im Verzug auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Die Sätze 1 bis 3 finden bei Auskunftsverlangen nach Absatz 1 Satz 2 keine Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. 5Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und 3 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. § 95 Absatz 2 gilt entsprechend".

[41] Respecto a los que engloba y no este deber de transmisión de información, puede verse KELLER/BRAUN, 2019, p. 75 y GRIMM, 2021, p. 487. En contra de la amplitud de este deber de colaboración parecen manifestarse VOSS/MÖLLER-BERTRAM, 2022, p. 319, al afirmar que las autoridades judiciales solamente tienen que confirmar la sospecha inicial de un delito para la recopilación de contraseñas y otros datos.

sona que preste o coopere en servicios de telecomunicaciones o servicios de telecomunicaciones para empresas debe proorcionar inmediatamente los datos necesarios[42]. Y añade que el apartado 2 del § 95 rige para estos casos. Por su parte, el § 95 StPO[43] establece la posibilidad de aplicar en contra del sujeto que se niegue a colaborar los medios administrativos y coercitivos regulados en el § 70 StPO[44].

De acuerdo con este precepto, a quien se niega a declarar o a prestar juramento de manera injustificada, se le imponen los costes ocasionados por su incomparecencia y, además, una multa administrativa (*Ordnungsgeld*) que, en caso de no poder ser cobrada, se convertirá en una pena privativa de libertad (*Ordnungshaft*). La multa será de un mínimo de 5 euros y un máximo de 1000, y la detención de un mínimo de 1 día y un máximo de 6 semanas (art. 6 de la Ley introductoria al Código penal, apartados 1 y 2)[45]. De acuerdo con el apartado 2 del § 70 StPO, es posible también ordenar la detención para forzar el testimonio. Sin embargo, esa detención no podrá tener una duración superior a la del propio proceso y, en ningún caso, será superior a seis meses.

Por lo tanto, y a modo de recapitulación: se podrá solicitar la información necesaria para la investigación de los hechos o para la determinación del paradero de un acusado; la solicitud de información resulta vinculante para quien proporciona o coopera en servicios de telecomunicaciones o servicios telemáticos, y ese deber implica, no solo la obligación de proporcionar los datos requeridos, sino de hacerlo *inmediatamente*. En caso de que el sujeto obligado se niegue a colaborar, en virtud del conjunto de remisiones de unos parágrafos a otros, puede ser aplicadas las medidas administrativas y coercitivas reguladas en el § 70 StPO, que establece las consecuencias de la negativa injustificada a testificar o prestar juramento, quedando expresamente excepcionadas de esa aplicación los sujetos eximidos del deber de declarar.

De este modo, en caso de que la persona requerida se niegue a colaborar, pueden serle aplicadas las mismas medidas que a aquellos que, estando obligados, se niegan a declarar o a prestar declaración *injustificadamente:* una multa o incluso prisión

[42] Agradezco al Profesor Luís Greco, amigo desde los ya lejanos años muniqueses, sus indicaciones sobre la regulación de este problema.

[43] § 95 StPO: "Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. 2. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind".

[44] § 70 StPO: (1) Wird das Zeugnis oder die Eidesleistung ohne gesetzlichen Grund verweigert, so werden dem Zeugen die durch die Weigerung verursachten Kosten auferlegt. 2. Zugleich wird gegen ihn ein Ordnungsgeld und für den Fall, daß dieses nicht beigetrieben werden kann, Ordnungshaft festgesetzt. (2) Auch kann zur Erzwingung des Zeugnisses die Haft angeordnet werden, jedoch nicht über die Zeit der Beendigung des Verfahrens in dem Rechtszug, auch nicht über die Zeit von sechs Monaten hinaus.

[45] Art. 6 EGStGB (Einführungsgesetz zum Strafgesetzbuch): "(1) Droht das Bundesgesetz Ordnungsgeld oder Zwangsgeld an, ohne dessen Mindest- oder Höchstmaß zu bestimmen, so beträgt das Mindestmaß fünf, das Höchstmaß tausend Euro. Droht das Landesgesetz Ordnungsgeld an, so gilt Satz 1 entsprechend. (2) Droht das Gesetz Ordnungshaft an, ohne das Mindest- oder Höchstmaß zu bestimmen, so beträgt das Mindestmaß einen Tag, das Höchstmaß sechs Wochen. Die Ordnungshaft wird in diesem Fall nach Tagen bemessen".

preventiva, con una duración limitada. Se trata de las llamadas "medidas coercitivas" del Derecho alemán que buscan, de manera similar a las medidas cautelares españolas[46], garantizar el éxito del proceso. Los presupuestos para la aplicación de la prisión preventiva están regulados en el § 112 StPO, y coinciden, al menos en gran parte, con los exigidos en nuestro Ordenamiento para decretar la prisión provisional de acuerdo con el art. 503 LECrim[47].

D) ***Italia***

En el Ordenamiento italiano, por su parte, el art. 256 del *Codice di Procedura Penale* (CPPit) ha regulado tradicionalmente el llamado "deber de exhibición y secreto". Como es sabido, la Ley n. 48, de 18 de marzo de 2008, por la que se ratifica y ejecuta el Convenio del Consejo de Europa sobre ciberdelincuencia elaborado en Budapest el 23 de noviembre de 2001, constituye el referente normativo en lo relativo a la investigación tecnológica, y contiene, entre otras cosas, normas para adaptación al Derecho interno. Esta Ley vino a reformar el art. 256 CPPit, dedicado al deber de exhibición y secreto[48]. Así, desde 2008, de acuerdo con el apartado 1 de dicho artículo, semejante deber alcanza también a los datos y programas informáticos[49], al establecerse que "las personas señaladas en los artículos 200 y 201 deberán entregar inmediatamente a la autoridad judicial, previa solicitud, las escrituras y documentos, incluso en original si así lo ordenare, (así como los datos, informaciones y programas informáticos, incluso mediante su copia en soporte adecuado) y cualquier otra cosa que tengan por razón de su cargo, ministerio, profesión o arte, a menos que declaren por escrito que se trata de secreto de Estado o secreto inherente a su oficio o profesión"[50]. Las personas señaladas en los arts. 200 y 201 CPPit son aquellas que están amparadas por el secreto profesional, pues en el art. 200 se cita expresamente a los abogados, sacerdotes, médicos, farmacéuticos y periodistas, y en el art. 201, por su parte, a los funcionarios para los que rige un deber de secreto. Por lo tanto, si ese deber, también en el ámbito de las nuevas tecnologías desde 2008, rige para un círculo de sujetos que en determinadas situaciones resultan eximidos de semejante obligación, ha de entenderse que dicho deber de colaboración

[46] Acerca de la naturaleza de estas medidas y del panorama en la doctrina alemana, SANDOVAL REYES, 2020, pp. 145 y ss.

[47] En concreto, el § 112 StPO lo permite si existen fuertes indicios de la comisión el delito y, además, un motivo para la detención, fundamentado éste en el riesgo de fuga, en la sospecha de que puedan falsearse o destruirse pruebas o influir en testigos, o en el riesgo de que se dificulte el descubrimiento de la verdad.

[48] Véase PAOLETTI, 2020, pp. 229 y ss.

[49] Cuestiones más concretas relativas al tipo de registro o de soporte pueden encontrarse en CANZIO/LUPARIA, 2018, pp. 230 y ss.

[50] Art. 256.1. CPP: "Le persone indicate negli artt. 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreti di Stato ovvero di segreto inerente al loro ufficio o professione ".

rige, desde luego, para todos aquellos que no se encuentran cubiertos por ninguna excepción.

El incumplimiento de ese deber de colaboración debe ser sancionado como un "incumplimiento de las disposiciones de la autoridad"[51], conforme al art. 650 del Código penal italiano (CPit)[52], que sanciona con pena de prisión de hasta tres meses o multa de hasta 206 euros a quien "no respete una medida legalmente dictada por la Autoridad por razones de justicia o seguridad pública, o de orden o higiene pública[53]". Se trata de una norma de carácter subsidiario, pues su aplicación procede solamente cuando el hecho no sea constitutivo de una infracción más grave. En el supuesto que tratamos procede aplicar este precepto "por razones de justicia", pues bajo esta denominación se agrupan los casos de desobediencia a jueces, fiscales y policía judicial que no constituyan otros delitos. Se trata de una "contravención" [54] y, por lo tanto, constituye una infracción menor de las denominadas *oblazionabile*; esto es, aquellas que son susceptibles de pago voluntario.

En el ámbito procesal, el término *oblazione* designa una forma de extinción de la pena, por medio del pago[55], fundada en razones de economía. El recurso a esta figura está permitido en dos tipos de contravenciones: las sancionadas con pena de multa preceptiva, contempladas en el art. 162 del CPit[56], y aquellas que llevan asociada una pena de multa, pero no como pena única, sino como alternativa, y que están reguladas en el art. 162 bis CPit[57]. Las primeras se califican de obligatorias, y las segundas, de

[51] Manifiesto mi gratitud al Profesor Francesco Diamanti, de la Universidad de Módena, por su orientación en esta materia.

[52] La constitucionalidad de este precepto ha sido fuertemente debatida, especialmente por su indeterminación. Véase, por ejemplo, PELLIZZONE, 2015, pp. 36 y ss.

[53] Las razones de higiene hacen referencia a emergencias sanitarias, como las situaciones de calamidad o epidemia. No en vano, este precepto que adquirió, como indica Fiorella, un inusitado protagonismo a raíz de la pandemia del COVID a principios de 2020, y su aplicabilidad fue discutida. Véase FIORELLA, 2021, pp. 134 y ss. y BAFFA, 2020, pp. 16 y ss.

[54] Como es sabido, en el Derecho penal italiano las infracciones penales (*reati)* se clasifican, según el tipo de pena que llevan aparejada, en delitos (*delitti*) y contravenciones (*contravenzioni)*. Los delitos tienen previstas, con carácter cumulativo o alternativo, penas principales de prisión perpetua (*ergastolo*), prisión (*reclusione*) y la multa (*multa)*, mientras que en las contravenciones las penas principales son de arresto (*arresto*) y/o multa contravencional (*ammenda)*. Véase CARDENAL MONTRAVETA, 2007, p. 5.

[55] Véase, por ejemplo: ALEO, 2008, p. 220.

[56] Art. 162. "Oblazione nelle contravvenzioni.

Nelle contravvenzioni, per le quali la legge stabilisce la sola pena dell'ammenda, il contravventore è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima del decreto di condanna, una somma corrispondente alla terza parte del massimo della pena stabilita dalla legge per la contravvenzione commessa, oltre le spese del procedimento.

Il pagamento estingue il reato.

[57] Art. 162-bis.

Oblazione nelle contravvenzioni punite con pene alternative.

Nelle contravvenzioni per le quali la legge stabilisce la pena alternativa dell'arresto o dell'ammenda, il contravventore può essere ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima del decreto di condanna, una somma corrispondente alla metà del massimo dell'ammenda stabilita dalla legge per la contravvenzione commessa, oltre le spese del procedimento.

Con la domanda di oblazione il contravventore deve depositare la somma corrispondente alla metà del massimo dell'ammenda.

discrecionales. Así, mientras que en las *oblazione* obligatorias se permite que el encausado o "indiciado" (equivalente al investigado en nuestro Derecho), antes de la apertura del juicio, o antes de que la sentencia sea firme, pague, además de las costas, la cantidad correspondiente a la tercera parte de la pena máxima establecida por la ley, quedando el Juez obligado a aceptar el pago, en las facultativas, el Juez decide si permite el pago, y en caso de aceptarlo, el encausado, con idéntico plazo al que rige en la obligatoria, ha de pagar la mitad del máximo de multa establecida para la infracción cometida, además de las costas. La *oblazione*, regulada en el art. 140 del CPPit, resulta inadmisible en determinados casos en los que el sujeto sea reincidente[58]. El incumplimiento que aquí analizamos constituye, en definitiva, una contravención susceptible de *oblazione* facultativa. De esta manera, si el Juez lo admite, el sujeto que se niega a colaborar podrá extinguir su infracción mediante el pago de 103 euros.

E) ***España***

En España, como es sabido, a pesar de las incontables recomendaciones y reclamaciones de distintos sectores[59], durante muchos años continuó llevándose a cabo la investigación tecnológica mediante la aplicación analógica de preceptos destinados a la investigación más clásica. Finalmente, tras una Sentencia del Tribunal Constitucional[60] que declararía la nulidad de unas comunicaciones y precipitaría la reforma, el legislador español llevó a cabo la ansiada reforma de la Ley de Enjuiciamiento Criminal operada por LO 13/2015, de 5 de octubre[61]. Entre otras muchas cosas, el legislador estableció una serie de deberes de cooperación sobre el sector privado, y sancionó su incumplimiento expresamente como un delito de desobediencia. La técnica legislativa empleada no resulta completamente satisfactoria, pues al regularse

L'oblazione non è ammessa quando ricorrono i casi previsti dal terzo capoverso dell'articolo 99, dall'articolo 104 o dall'articolo 105, né quando permangono conseguenze dannose o pericolose del reato eliminabili da parte del contravventore.

In ogni altro caso il giudice può respingere con ordinanza la domanda di oblazione, avuto riguardo alla gravità del fatto.

La domanda può essere riproposta sino all'inizio della discussione finale del dibattimento di primo grado.

Il pagamento delle somme indicate nella prima parte del presente articolo estingue il reato".

[58] Véase al respecto, por ejemplo, BONTEMPELLI, 2015, pp. 473 y ss.

[59] Puede verse una exposición detallada del panorama anterior a la reforma y su problemática en MARCHENA GÓMEZ/ GONZÁLEZ-CUÉLLAR SERRANO, 2015, pp. 174-194.

[60] La STC 145/2014, de 22 de septiembre (ECLI:ES:TC:1984:114), declaró la nulidad de unas grabaciones obtenidas mediante la colocación de micrófonos en la celda de una comisaría por considerar que dicha medida de investigación vulneraba el derecho al secreto de las comunicaciones, poniendo de manifiesto que no existía una ley orgánica que diera cobertura al sacrificio de ese derecho. Esta sentencia se sumaba a la del TJUE de 8 de abril de 2014, que exigía la referencia al principio de proporcionalidad a la hora de regular la conservación de datos y el acceso a los mismos por parte de los poderes públicos. Véase MARCHENA GÓMEZ/ GONZÁLEZ-CUÉLLAR SERRANO, 2015, pp. 180 y 194.

[61] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

esos deberes al hilo de cada medida de investigación particular, parece que el contenido de las obligaciones varía sustancialmente según la medida de investigación que se lleve a cabo.

Este deber de colaboración se establece, en primer lugar, sobre los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como sobre todo sujeto que medie en el proceso de comunicación, facilitándolo (art. 588 ter e. 1. LECrim). El incumplimiento da lugar a un delito de desobediencia, de acuerdo con el apartado 3 del art. 588 ter e LECrim. Por su parte, el art. 588 sexies c. LECrim, dentro del aparatado dedicado al registro directo de dispositivos de almacenamiento masivo de datos, permite a las autoridades y agentes encargados de la investigación ordenar a cualquier persona conocedora del funcionamiento del sistema informático o de 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". Asimismo, de acuerdo con el art. 588 septies b. LECRim, dedicado al registro remoto de equipos informáticos, tanto los sujetos mencionados en el art. 588 ter e. LECrim como "los titulares o responsables del sistema informático o base de datos objeto del registro", quedan sujetos al deber de "facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema". También pesa sobre ellos la obligación de "facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización". Además, de acuerdo con el apartado 2, las autoridades y los agentes al cargo de la investigación pueden 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 para el buen fin de la diligencia". Este deber da lugar a la misma responsabilidad que en el caso del 588 ter e. LECrim, es decir, a un posible delito de desobediencia. Por último, de acuerdo con el art. 588 octies LECrim, cualquier persona física o jurídica puede ser requerida por el Ministerio Fiscal o por la Policía Judicial para que conserve datos concretos incluidos en un sistema de información que se encuentre a su disposición hasta que se obtenga la pertinente orden judicial. El requerido queda sujeto a la responsabilidad establecida en el apartado 3 del art. 588 ter LECrim, por lo que en caso de incumplimiento del deber de colaborar o de guardar silencio incurrirá también en un delito de desobediencia.

La constante referencia a la desobediencia en los deberes de colaboración de acuerdo con la actual regulación de la LECrim desaparece en gran parte en el texto del Anteproyecto de Ley de Enjuiciamiento Criminal, aprobado por Consejo de Ministros el 24 de noviembre de 2020. Así, en el art. 361 del Anteproyecto, dedicado a

los deberes de colaboración de empresas de telefonía, operadores de telecomunicaciones y prestadores de servicios de la sociedad de la información, esta referencia se ha eliminado. En el registro de dispositivos de almacenamiento masivo de información, se dedica el art. 428 a los deberes de colaboración y ahí, no obstante, se mantiene la referencia al apercibimiento de incurrir en delito de desobediencia. Pero en el art. 432, dedicado al deber de colaboración en el registro remoto, vuelve a suprimirse la alusión a la posibilidad de incurrir en el delito de desobediencia. Y lo mismo ha sucedido en las medidas de aseguramiento relativas a la conservación de datos, que mantiene el correspondiente deber de colaboración en el art. 435 del Anteproyecto, pero guarda silencio ahora respecto a la sanción que correspondería en caso de incumplimiento.

En definitiva: tras la reforma de la LECrim en lo relativo a las medidas de investigación tecnológica operada en 2015, se instaura una serie de deberes de colaboración sobre determinados sujetos[62] y su incumplimiento se castiga, pues así lo dice la propia LECrim, a través del delito de desobediencia. La referencia a esta sanción desaparece en el Anteproyecto de LECrim de 2020, salvo en el registro directo de dispositivos de almacenamiento masivo de datos, donde se mantiene. En todo caso, sea como fuere, lo cierto es que, fuera del ámbito procesal y penal, numerosas normas se han ocupado de establecer deberes de colaboración sobre sujetos privados en distintos sectores, cuyo incumplimiento ha sido sancionado con la imposición de cuantiosas multas. Citaremos algunas de ellas.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, dedica dos artículos a una serie de deberes de colaboración (los arts. 11 y 36), aunque realmente, los deberes de colaboración que nos interesan son introducidos por la Disposición adicional novena añadida por la disposición final 2.16 de la Ley 9/2014, de 9 de mayo. En dicha norma, bajo el título "Gestión de incidentes de ciberseguridad que afecten a la red de Internet", se establece en el art. 2 el deber de los prestadores de servicios de la Sociedad de la información de suministrar – con el límite del respeto al secreto de las comunicaciones-, la información necesaria al CERT[63] competente y a las autoridades para la gestión de los incidentes de ciberseguridad, incluyendo, según reza el artículo, "las direcciones IP que puedan

[62] Se excepciona del deber de colaboración tanto en el registro remoto (art. 588 septies b. 2 LECrim) como en el registro directo (art. 588 sexies c. 5 LECrim) 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 LECrim, no pueden declarar en virtud del secreto profesional. La cuestión relativa a los sujetos excepcionados en la LECrim -los mencionados y los olvidados-, la analicé en otro artículo (2021, pp. 1-44).

[63] Como se indica en el glosario del Instituto Nacional de Ciberseguridad (INCIBE), CERT es el acrónimo en inglés de "Computer Emergency Response Team" (equipo de respuesta ante emergencias informáticas en español). Se trata del equipo de expertos encargados, tanto de la prevenir incidencias de seguridad en redes de comunicaciones y sistemas informáticos, como de ofrecer respuestas cuando estas incidencias llegan a producirse.

Véase: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf, última consulta 9-3-22.

hallarse comprometidas o implicadas en los mismos". Por su parte, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, aparece plagada de deberes de colaboración, y califica como infracción grave -sancionable con una multa de hasta 2 millones de euros, según el art. 79- la negativa a ser inspeccionado o "la no colaboración con la inspección cuando ésta sea requerida y la no identificación por la persona física o jurídica que tenga la disponibilidad de los equipos e instalaciones o sea titular de la finca o inmueble en donde se ubican los equipos e instalaciones". También la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece en su art. 52 un deber de colaboración con la Agencia Española de Protección de Datos que engloba a "las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares", quedando estos sujetos obligados a proporcionar los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación, bajo amenaza de incurrir en una infracción muy grave[64]. Por su parte, la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves obliga a las empresas de transporte aéreo, los operadores de las aeronaves y las entidades de gestión de reserva de vuelos a proporcionar los datos de Registro de datos de Pasajeros (PNR), bajo amenaza de sanción económica de hasta 300.000 euros. Y en ese mismo sentido, resulta especialmente destacable la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que regula, por su parte, el deber de colaboración de las Administraciones públicas y de cualquier persona física o jurídica, consistente en proporcionar a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial todos aquellos datos -informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas- que pueden ser obtenidos sin la exigencia de una autorización judicial (art. 7.3). Es decir, rige esta Ley para la información relativa a la investigación que no exija una autorización de un juez, y que queda fuera del ámbito de aplicación de la LECrim. La negativa a cooperar proporcionando la información requerida se considera una infracción muy grave según el art. 58 j. y es susceptible de ser sancionada con una multa de 360.0001 a 1.000.000 de euros.

[64] De acuerdo con el art. 52, letra ñ, constituye una infracción muy grave "no facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación". La determinación del importe de las sanciones se realiza mediante una remisión al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Texto disponible en: https://www.boe.es/doue/2016/119/L00089-00131.pdf, última consulta: 10-3-22.

Por último, y simplemente para poner de manifiesto otra diferencia con la regulación en el Ordenamiento jurídico francés, nos gustaría hacer una pequeña observación sobre la inexistencia de agravantes genéricas aplicables a los delitos en los que se utiliza un sistema informático por el hecho de disponer de medios de cifrado y, en general, por contribuir en cierto modo a la comisión o a la impunidad del delincuente gracias al anonimato y la deslocalización propias del ciberespacio[65]. Un repaso superficial permite distinguir que no hay agravante genérica a la que reconducir este fenómeno en la regulación actual. Las que aparentemente tendrían un mayor encaje serían las del art. 22.2 CP. Sin embargo, las tres deben ser rechazadas.

No se ejecuta el hecho mediante disfraz, pues de acuerdo con jurisprudencia reiterada, en la aplicación de la agravante de disfraz han de concurrir una serie de requisitos: uno objetivo, consistente en la utilización de un medio apto para desfigurar la apariencia externa de una persona[66], uno cronológico, que exige que el disfraz se utilice durante la ejecución del delito, y otro subjetivo, de manera que ha de estar "vinculada al propósito preordenado de hacer imposible o dificultar la identificación del autor"[67]. Por lo tanto, en los delitos cometidos que guardan conexión con un sistema informático no puede entenderse que existe agravante de disfraz por el uso de ese sistema al no existir un medio apto para desfigurar el rostro o la apariencia externa, pues ello supondría una interpretación analógica *contra reo* inadmisible.

Tampoco procede aplicar una agravante de abuso de superioridad sin mayor fundamentación.

La agravante que más posibilidades de ser aplicada presenta sería la relativa a la ejecución del hecho "aprovechando las circunstancias de lugar (…) que (…) faciliten la impunidad del delincuente" cuando el delincuente se vale de la deslocalización espacial para garantizarse la impunidad que le proporciona el sistema informático, frente a otro modo de comisión tradicional, mucho más arriesgado. La aplicación de semejante agravante no se plantearía, en ningún caso, en los ciberdelitos en sentido estricto -en el allanamiento informático del 197 bis CP o en el sabotaje informático

[65] Cuestión distinta es el mayor desvalor de resultado que puede conllevar la utilización de estos medios y que ya ha sido tenido en cuenta puntualmente por el legislador. En este sentido, subraya acertadamente CARUSO FONTÁN (2019, p. 7) la incorporación, con la reforma de 2015, de un tipo cualificado al delito de incitación al odio o a la violencia racial, al establecerse en el apartado 3 del art. 510 CP que las penas previstas en los apartados anteriores se impondrán en su mitad superior "cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas". Existen otras referencias a la utilización de las nuevas tecnologías. Por citar algún ejemplo: el art. 183 ter CP hace referencia a la utilización de un medio tecnológico en sus apartados 1 y 2 cuando castiga el contacto con el menor de dieciséis realizado a través de "internet, del teléfono o de cualquier otra tecnología de la información y la comunicación"; en el art. 578. 2 CP, la utilización de estas tecnologías es tenida en cuenta también para agravar el delito de enaltecimiento o justificación del terrorismo; y tras la reforma operada por LO 8/2021, el artículo 189 bis CP pasa a castigar la distribución y la difusión de determinados contenidos a través las tecnologías de la información o de la comunicación.

[66] Por todas, STS 670/2005, de 27 de mayo (ECLI:ES:TS:2005:3407), FJ. 4.

[67] Así lo recuerda la STS 323/2021, de 27 de abril (ECLI:ES:TS:2021:1389), que aplicó la agravante de disfraz en un robo con violencia o intimidación perpetrado con mascarilla cuando su uso no era obligatorio.

del 264 CP-, puesto que, al tratarse de delitos cometidos *contra* un sistema informático, solamente pueden realizarse en el ciberespacio. De esta manera el espacio virtual se convierte en un elemento inherente al delito, faltando entonces el elemento subjetivo que requiere el aprovechamiento. Por lo tanto, la aplicación de la agravante solamente sería posible en los ciberdelitos en sentido amplio, pues estamos ante delitos tradicionales que pueden ser cometidos a través de un sistema informático para, esta vez sí, "aprovechar" la impunidad que proporciona esta forma de comisión. No obstante, parece claro que el legislador no estaba pensando en esa opción cuando incluyó tal agravante, por lo que considerar el espacio virtual como un lugar en sí mismo supone una analogía *contra reo* inadmisible. Cosa distinta es que en el futuro quepa replantearse la posibilidad de considerar el ciberespacio un lugar[68] y, además, uno de esos que facilitan la comisión de un delito. Respecto a esta circunstancia, querríamos destacar una reciente sentencia de la Audiencia Provincial de Barcelona (SAP de Barcelona 653/2019, de 29 de mayo, ECLI:ES:APB:2019:14581), que revoca parcialmente la Sentencia 243/2019, del Juzgado de lo penal n. 9, de Barcelona (ECLI:ES:JP:2019:29). La titular del Juzgado había condenado a un *youtuber* que se había grabado dando de comer a un mendigo unas galletas con pasta de dientes en su interior, por un delito contra la integridad moral a una pena de 15 meses de prisión. Le imponía, además, de acuerdo con el art. 49 CP, la prohibición de acudir durante cinco años al lugar donde se había cometido el delito, entendiendo como tal -y esto es lo llamativo de la sentencia- la red social de *Youtube* donde se colgó el vídeo en el que se vejaba al mendigo. La Audiencia Provincial de Barcelona estimó parcialmente el recurso y suprimió esta prohibición, argumentando que el lugar donde se cometió el delito fue la vía pública donde se encontraba el mendigo, y que el art. 48 "no puede interpretarse de manera extensiva ni analógicamente en contra del reo para sustentar la prohibición de acceder a la Red Social Youtube"[69]. Lógicamente, compartimos la argumentación de la Audiencia Provincial de Barcelona. Pero también creemos que, en esta nueva dimensión constituida por el ciberespacio y sus nuevas realidades, conviene repensar no solo la parte especial, sino también la parte general del Código penal[70].

Por lo tanto y, en definitiva, aunque ninguna agravante genérica resulta de aplicación en los ciberdelitos en sentido amplio de acuerdo con la actual regulación del Código penal, en una futura reforma no parece descabellada su introducción. En este sentido, no puede perderse de vista que, a pesar de que la agravante del art. 22.2 CP resulta controvertida debido a que tanto tratar de facilitar la ejecución del delito como conseguir la impunidad pueden considerarse inherentes a la realización misma del

[68] Acerca de la posibilidad de plantear el ciberespacio como un nuevo ámbito de comisión delictiva, reflexiona CARUSO FONTÁN, 2019, pp. 5-7.

[69] SAP de Barcelona 653/2019, de 29 de mayo (ECLI:ES:APB:2019:14581), FJ. 4.

[70] A favor de que el Derecho no se mantenga al margen de lo que sucede en el ciberespacio ya MARCHENA GÓMEZ, 2001, pp. 163-165.

delito -además de resultar esta última contraria a la impunidad del autoencubrimiento-, lo cierto es que si se mantiene una agravante como ésta en el Código penal, sea cual sea la fundamentación que para ella se sostenga –y es diversa la que proporciona la doctrina[71] - la misma parece extensible a la comisión de delitos a través de los sistemas informáticos.

En cualquier caso, aunque no disponemos de una agravante genérica, sí existe en el Código penal una agravante específica de este tenor en los delitos de organizaciones y grupos criminales, pues el legislador ha tenido a bien aumentar la pena, imponiéndola en su mitad superior, cuando las organizaciones o los grupos criminales dispongan "de medios tecnológicos avanzados de comunicación o transporte que por sus características resulten especialmente aptos para facilitar la ejecución de los delitos o la impunidad de los culpables", contemplándose esta cualificación en los arts. 570 bis 2. c) y 570 ter 2. c), respectivamente.

3. **El delito de desobediencia como respuesta**

Tal y como hemos indicado, en la actual regulación de los deberes de colaboración de la LECrim se hace referencia a la sanción de su incumplimiento a través del delito de desobediencia. El texto del Anteproyecto de LECrim de 2020, por el contrario, suprime esas referencias y solamente mantiene el apercibimiento por este delito en el registro de dispositivos de almacenamiento masivo de información del art. 428.

Sea como fuere, existiendo una orden, como sucede aquí, el incumplimiento resulta, en cualquier caso, reconducible al delito de desobediencia, lo diga o no la normativa procesal[72], y ello con independencia de que el bien jurídico protegido en este delito se configure como el tradicional principio de autoridad, que resulta quebrado, como el correcto funcionamiento de los servicios y funciones públicas o, según se ha sostenido en tiempos más recientes, como la dignidad de la función pública ordenada al correcto funcionamiento de la Administración Pública entendida en términos democráticos[73].

Como es sabido, en nuestro Derecho contamos con dos delitos de desobediencia principales que, según recordaba Quintero[74], únicamente se parecen en el nombre,

[71] Así, unos autores encuentran su fundamento en la superioridad del sujeto activo o en la mayor vulnerabilidad de la víctima, mientras que la jurisprudencia, vacilante, unas veces acude a la mayor reprochabilidad del hecho y otras a la mayor energía criminal empleada. Véanse todas estas opiniones en GARCÍA PLANAS, 1999-2000, pp. 36-39, quien, además, se manifiesta en contra del mantenimiento de esta agravante (p. 36). También se pronuncia claramente en contra, DOPICO GÓMEZ-ALLER, 2011, p. 87.

[72] A pesar de que en tiempos del Covid parece que el Ejecutivo no ha tenido claro que no procede castigar por desobediencia cuando la desobediencia es a la norma, y no a un mandato u orden específicos. Véase a este respecto ALONSO RIMO, 2020, pp. 85-110.

[73] Una exposición de las distintas tesis mantenidas, casi autor por autor, en LORENTE VELASCO, 2010, pp. 55-66.

[74] QUINTERO OLIVARES, 2021, p. 1.

pues uno hace referencia a la de los funcionarios respecto de las órdenes de sus superiores jerárquicos y afecta al funcionamiento de la administración pública (art. 410 y ss. CP), y el otro se incluye como delito contra el orden público, situándose entre la sedición y los desórdenes públicos (art. 556 CP). Por razón del sujeto activo, la desobediencia aplicable en nuestro caso sería la desobediencia de los particulares del art. 556 CP. Así, el art. 556 CP, tras la modificación llevada a cabo por LO 1/2015, de 30 de marzo, castiga con pena de prisión de tres meses a un año o multa de seis a dieciocho meses, a quienes, "sin estar comprendidos en el artículo 550, resistieren o desobedecieren gravemente a la autoridad o sus agentes en el ejercicio de sus funciones, o al personal de seguridad privada, debidamente identificado, que desarrolle actividades de seguridad privada en cooperación y bajo el mando de las Fuerzas y Cuerpos de Seguridad". En un segundo párrafo se castiga como delito leve y con la pena de multa de uno a tres meses a quienes faltaren al respeto y consideración debida a la autoridad, en el ejercicio de sus funciones.

La desobediencia aquí analizada es la sancionada en el art. 556.1 CP, no siendo de aplicación el art. 550 CP, del que el propio art. 556.1 se declara subsidiario, pues no se da la necesaria agresión o resistencia grave con intimidación o violencia que exige el tipo. Para que la conducta sea constitutiva de delito se exigen una serie de requisitos[75] cuya concurrencia puede afirmarse aquí, sin lugar a dudas: existe una orden concreta y expresa dirigida a un ciudadano o conjunto de ciudadanos, emitida por la Autoridad o sus agentes en el ejercicio de sus funciones, revestida de las formalidades necesarias y notificada al sujeto llamado a obedecerla, siendo éste requerido de alguna manera, de forma personal y directa. Todas estas condiciones se cumplen cuando un juez ordena a un sujeto a colaborar en la investigación, pues esa orden judicial constituye el requerimiento personal, revestido de las formalidades legales oportunas. Concurre, por lo demás, dolo de desobedecer, pues frente al mandato de la autoridad, el obligado a cumplirlo manifiesta una oposición clara y contumaz. Lo único que resultaría discutible es la gravedad de la desobediencia, que sin duda se dará si atendemos a la importancia de la orden. Sin embargo, si para su calificación como tal se exige un especial grado de oposición[76], en el sentido de una desobediencia pertinaz y reiterada[77], habrá que esperar a que la negativa a colaborar se repita,

[75] Por todas, SSTS 821/2003, de 5 de junio (ECLI:ES:TS:2003:3859) y 1219/ 2004, de 10 de diciembre (ECLI:ES.TS.2004:8004).

[76] En contra de considerar que la gravedad de la desobediencia ha de medirse por el contenido de la orden se manifiesta un amplio sector doctrinal. Así, por ejemplo, ya LORENTE VELASCO, 2010, p. 263, calificaba como "altamente arriesgado" el criterio de atender al bien jurídico protegido por la orden. En tiempos más recientes, entre otros, ALONSO RIMO, 2020, pp. 108, afirma que atender al contenido de la orden supone confundir el objeto de tutela del delito de desobediencia con el objeto tutelado por la propia orden incumplida, y BOCANEGRA MÁRQUEZ, 2022, p. 27, por su parte, argumenta que semejante entendimiento supone un *bis in ídem*, pues el delito de desobediencia constituiría entonces un instrumento de reforzamiento de la tutela del bien jurídico.

[77] Por todas, la STS 485/2002, de 14 de junio (ECLI:ES:TS:2002:4367).

como de hecho ha sucedido con la multinacional Apple ante los requerimientos judiciales obtenidos por el FBI en EEUU.

Ahora bien, la sanción por medio del delito de desobediencia plantea dos problemas de distinto orden a los que nos gustaría hacer mención. Uno hace referencia a la entidad de la pena y, en concreto, a su escaso efecto disuasorio; el otro, tiene que ver con los sujetos a quienes no se puede imponer esa pena y, en particular, a la imposibilidad de que las personas jurídicas incurran en un delito de desobediencia. Tras ello, haremos referencia a posibles respuestas ante el incumplimiento por parte de las empresas tecnológicas, para terminar con una exposición de los inconvenientes de un abordaje penal frente a uno administrativo.

A) *La ineficacia de una pena que no intimida*

Como ya hemos señalado, la sanción a imponer a una persona física que comete una desobediencia grave es una pena de prisión de tres meses a un año o, alternativamente, una multa de seis a dieciocho meses. Por lo tanto, a la hora de elegir, con frecuencia el juez optará por la multa, especialmente si tenemos en cuenta que la de prisión es inferior a dos años. Como la multa no es proporcional, sino que sigue el sistema días multa, la cuantía dependerá de la situación económica del reo, pudiendo alcanzar un tope de 400 euros/día. De acuerdo con ello, el máximo que se puede alcanzar será de (400x30x18) 216.000 euros.

Si el juez optara por la pena de prisión, lo normal será que suspenda su ejecución cuando concurran los requisitos del art. 80 CP. Y en este sentido, cabe hacer una mínima reflexión a modo de recordatorio acerca de los fines de la pena: las penas no superiores a dos años, como ésta, ponen en jaque el efecto intimidatorio que el castigo ha de ejercer sobre el ciudadano.

Sin pretender realizar un análisis en profundidad de las condiciones y efectos de la suspensión de la pena -institución que, como es sabido, ha sufrido una importante reforma en el año 2015-, baste realizar unas mínimas consideraciones, susceptibles, eso sí, de numerosos matices y puntualizaciones: una pena que se cree que va a ser suspendida resulta inocua desde el punto de vista de la prevención general negativa, que constituye, por lo demás, si no el principal, desde luego uno de los más importantes fines de la pena.

En efecto, parece posible aceptar que los sujetos -o la mayor parte de ellos- toman decisiones racionales que le resultan provechosas, y que ese provecho o utilidad depende de que sea positivo el saldo resultante de restar a los beneficios derivados de una conducta los costes que la misma supone[78]. A la hora de cometer un delito, esos costes son calculados por el ciudadano de acuerdo con el cruce de dos coordenadas:

[78] Acerca de la intimidación de la pena como manifestación de la racionalidad, véase, por ejemplo: CARDENAL MONTRAVETA, 2015, p. 5 y ss.

la que deriva de su percepción acerca de la probabilidad de ser descubierto, y la resultante de su apreciación acerca de la severidad de la pena a imponer. Por eso tiene un efecto tan negativo el hecho de que la pena no sea superior a dos años: no tanto porque efectivamente se suspenda, como porque el ciudadano sabe que esa suspensión se producirá con toda probabilidad, pues forma parte de la creencia popular el hecho de que las penas no superiores a dos años han sido tradicionalmente objeto de un tratamiento especial, y que no se ejecutan cuando el sujeto se estrena como delincuente -aunque, tal y como se establece en el art. 80.3 CP ni la suspensión ha de darse necesariamente, ni es requisito indispensable la no reiteración delictiva-.

Podemos, en consecuencia, afirmar que es limitado el efecto intimidatorio de la pena de la desobediencia porque, o bien es de multa, y la cuantía no es elevada, o bien es una de prisión que normalmente se suspenderá. Y, además, al margen de la entidad de castigo, lo cierto es que poco puede hacer la pena dirigida a un individuo para que una compañía de las dimensiones de Samsung o Apple tome una decisión respecto a uno de sus productos. Por eso nos atrevemos a aventurar que, con toda probabilidad, la amenaza del Juez de Instrucción en el caso de la tarjeta de Dina Bousselham no fue lo que decidió a Samsung a colaborar, sino que seguramente fueron cuestiones económicas, relacionadas con los costes reputacionales de la marca, las que llevaron a la adopción de una decisión semejante.

B) ***La imposibilidad de castigar a personas jurídicas por un delito de desobediencia***

Nos gustaría realizar aquí una breve reflexión acerca de los destinatarios de la sanción por incumplimiento del deber de colaborar. La negativa a cooperar con el investigador criminal proviene normalmente de las grandes empresas tecnológicas, pues es a ellas a quienes se recurre para acceder a un dispositivo cuando al investigador le resulta imposible, con la esperanza de que, habiendo creado el dispositivo, dispongan de un mayor conocimiento o de unos medios más avanzados para acceder a esa información. Y, sin embargo, el delito de desobediencia no es uno de aquellos que puede de ser cometido por una persona jurídica, por lo que paradójicamente no podrá sancionarse a la multinacional que se niegue a colaborar, incluso, como sucede con Apple, aunque esa actitud desafiante frente al sector público le reporte enormes beneficios económicos.

En efecto, la desobediencia no fue uno de los delitos por los que optó el legislador de 2010 al introducir la polémica responsabilidad penal de la persona jurídica, pues en el catálogo *numerus clausus* de delitos existente, de acuerdo con el art. 31 bis de CP, este delito no figuraba. Como es sabido, ese listado ha sufrido diversas ampliaciones con las sucesivas reformas del Código penal: la LO 3/2010, de 28 de enero realizó una pequeña ampliación, la LO 6/2011, de 30 de junio, incluiría el contrabando, la LO 1/2015, de 30 de marzo, la extendería a varias categorías delictivas, entre los que se encontraban diversos ataques a los sistemas de información, como

la interceptación de transmisiones no públicas de datos informáticos, la producción, adquisición o distribución de herramientas para acceder a un sistema de información, el sabotaje informático; y, por último, también la LO 1/2019, de 20 de febrero, ha hecho lo propio, realizando diversos desarrollos en tantos tipos penales que no pueden ser citados aquí[79]. Sin embargo, y a pesar de todas estas oportunidades que, como vemos, ha tenido el legislador, nunca ha incluido el delito de desobediencia como uno de los de posible comisión por personas jurídicas[80].

Esto explica que en el caso Dina Bousselham el juez instructor amenazara con incurrir en delito de desobediencia, como indicamos más arriba, al Director del Departamento de Asesoría jurídica de Samsung Electronics Iberia. En todo caso, como ya hemos dicho, resulta llamativamente escasa la pena, pues la sanción de la desobediencia, aun siendo grave, se reduce a una pena de prisión de tres meses a un año o multa de seis a dieciocho meses.

4. **Posibles soluciones *de lege ferenda* ante el incumplimiento de las multinacionales tecnológicas**

Ante este panorama cabe plantearse cuál es la opción legislativa más adecuada para sancionar este incumplimiento, especialmente si tenemos en cuenta que en este momento nos encaminamos, ni más ni menos, que hacia la elaboración de un nuevo Ciberconvenio[81]. En efecto, el 26 de mayo de 2021 la Asamblea General de la ONU aprobó en Nueva York la resolución 75/282 relativa a la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos[82]. Y como se espera que en esas negociaciones se aborden temas relacionados con la normativa y la competencia de la Unión Europea en el ámbito de la ciberdelincuencia, 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

[79] Una referencia detallada a estos tipos penales y a todos los de las sucesivas reformas puede encontrarse en ABEL SOUTO, 2021, pp. 4-12.

[80] Las paradojas no se limitan a la no inclusión de la desobediencia; baste recordar, por ejemplo, que tampoco están incluidos en el catálogo de delitos de posible comisión por personas jurídicas los delitos contra los derechos de los trabajadores.

[81] Así lo augura GARCÍA MENÉNDEZ, 2021, p. 8. Como indica este autor, el camino no ha estado exento de recelos, oponiéndose diversos sectores desde distintos frentes: la propia España, después EEUU, y posteriormente el sector tecnológico, con un manifiesto en contra a cargo de *Cybersecurity Tech Accord* y *Cyberpeace Institute*.

[82] La Asamblea General de la ONU decidió la creación de un comité *ad hoc* que, a partir de enero de 2022, debía convocar al menos seis sesiones y, además, una sesión de clausura en la que se presentaría un proyecto de Convenio a la Asamblea General de la ONU en 2024. El 20 de enero de 2022, la Asamblea General decidió posponer la primera sesión debido a la pandemia de COVID-19.

con fines delictivos" [83]. Con ello se pretende, como se indica en la propia Recomendación, no sólo crear nuevas normas comunes de la UE[84] para luchar contra la ciberdelincuencia, sino también medidas procesales que garanticen la cooperación entre Estados.[85]

Por lo tanto, con la posible sustitución del Convenio de Budapest, se impone la necesidad de repensar la solución que se da en los distintos Ordenamientos al fenómeno del incumplimiento de las empresas tecnológicas y plantear la posibilidad de adoptar alguna medida conjunta, al menos en el ámbito europeo, para dar una respuesta unitaria y eficaz a este tipo de desobediencia.

A) *Un abordaje penal: la desobediencia genérica o específica como delito susceptible de ser cometido por personas jurídicas*

Si se opta por un abordaje penal de este problema, la respuesta ha de venir de mano de la desobediencia, pues lo diga o no la LECrim, estamos ante la intermediación de una orden que es incumplida. Puede recurrirse a la aplicación del delito de desobediencia genérica, como se viene haciendo, y reformar el catálogo de delitos susceptibles de ser cometidos por personas jurídicas para incluir este delito entre ellos. En el caso de que se considerara inadecuada e insuficiente la pena establecida en el delito de desobediencia genérica, sería igualmente posible optar por la creación de un tipo de desobediencia específico. Eso es lo que se ha hecho en Francia, y esa misma opción ha sido la seguida por el legislador español en diversas ocasiones respecto de otras materias. No en vano, el Código penal español presenta otros muchos tipos de desobediencias específicas que castiga -aunque sorprendentemente no siempre[86]- con una pena superior: baste traer a colación la obstrucción de las labores de inspección y control de las sociedades sometidas a supervisión administrativa (art.

[83] Texto disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52022PC0132&from=EN, última consulta: 9-3-22.

[84] Además de las ya existentes, entre las que están la Directiva 2011/93/UE relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía; la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información; y la Directiva (UE) 2019/713 sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

[85] Como indica la Resolución, en la UE actualmente existen instrumentos de ejecución forzosa y cooperación judicial, "como la Directiva 2014/41/UE relativa a la orden europea de investigación en materia penal, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea 18, el Reglamento (UE) 2018/1727 sobre Eurojust, el Reglamento (UE) 2016/794 sobre Europol , el Reglamento (UE) 2017/1939 por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea 21, la Decisión marco 2002/465/JAI del Consejo sobre equipos conjuntos de investigación, y la Decisión marco 2009/948/JAI del Consejo sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales. También son pertinentes las propuestas de la Comisión de abril de 2018 sobre el acceso transfronterizo a las pruebas electrónicas 24 y el paquete de cooperación policial, que actualmente está tramitándose con arreglo al procedimiento legislativo de la UE. En el exterior, la Unión Europea ha celebrado una serie de acuerdos bilaterales con terceros países, como los acuerdos de asistencia judicial entre la Unión Europea y los Estados Unidos de América y entre la Unión Europea y Japón".

[86] Véase la crítica a la inferior pena del delito de impago de pensiones en ÁLVAREZ GARCÍA, 2007, p. 19.

294 CP), la desobediencia a órdenes expresas de subsanación por parte de la Administración en materia de explosivos (art. 348.4 c. CP), la desobediencia a órdenes expresas de la autoridad administrativa de corrección o suspensión de las actividades industriales no autorizadas (art. 327 b. CP), la desobediencia a la orden de someterse a pruebas de alcoholemia (art. 383 CP), la desobediencia a la resolución de la privación del permiso de conducir (art. 384 CP), la incomparecencia a citaciones judiciales (art. 463 CP) y la falta de comparecencia a comisiones de investigación (art. 502 CP), entre otras. Un tipo cualificado como ése podría incluirse, de considerarse pertinente, en el listado de delitos de los que deriva responsabilidad penal para las personas jurídicas.

A favor de la primera opción se pronuncian dos expertos en el ámbito del Derecho y las nuevas tecnologías, como son Eloy Velasco Núñez y Beatriz Saura Alberdi[87]. Proponen incorporar la desobediencia al catálogo de delitos susceptibles de ser cometidos por personas jurídicas, justamente "para evitar situaciones como la ocurrida en Estados Unidos con una multinacional de servicios informáticos, que ha desobedecido una resolución judicial en la que se le requería la cesión de datos de un teléfono móvil propiedad de un terrorista." En este sentido, afirma Velasco Núñez que "la negativa de Apple a colaborar y a cumplir un mandamiento de una Juez californiana (…) no tendría cobertura legal en España, y nos alerta frente a actitudes semejantes de invasión del poder judicial –que pretendía con esta cesión ver si el terrorista contó con cómplices, si se tenían previstas otras posibles acciones terroristas para evitarlas y dar con elementos de pruebas sobre la acción criminal así investigada-, posicionándonos a favor de que, en un futuro próximo, se confeccione una tabla de derechos de nueva generación que predicar no ya tanto contra el Estado, sino frente a esas multinacionales cuasi monopolísticas que, en la protección de su negocio, atentan contra derechos básicos –como el de la seguridad- de la sociedad, ante excepciones a la encriptación de telecomunicaciones y datos, que no tienen justificación ni proporcionalidad alguna"[88].

Compartimos punto por punto la crítica realizada por Velasco y Saura, pero diferimos de la solución propuesta. Estamos de acuerdo en que el actual incumplimiento de las multinacionales resulta inadmisible: no puede confiarse a la voluntad privada esa colaboración que requiere la investigación tecnológica, pues lo que de ningún modo ha de permitirse es que los intereses económicos de las empresas tecnológicas ni tampoco un ilimitado derecho a la intimidad cuya protección falsa e interesadamente enarbolan, genere un espacio de impunidad en el que le sea vetado el acceso al investigador criminal. Resultan plenamente aplicables aquí las palabras del Prof.

[87] Véase VELASCO NÚÑEZ/ SAURA ALBERDI, 2016, p. 83. Ambos autores proponen, por razones sustantivas, convertir en delitos susceptibles de ser cometidos por persona jurídica tanto el quebrantamiento de condena del art. 468 CP, como el delito de desobediencia del art. 556 CP.

[88] VELASCO NÚÑEZ, 2016, p. 103.

Álvarez García[89] a propósito de la sanción del delito de desobediencia: "no es aceptable el dejar de castigar esos comportamientos que se dirigen, en definitiva, contra el «fruto» del funcionamiento mismo del Estado de Derecho. La dejadez en cualquiera de esos casos supone la causación de un daño persistente y difícilmente reparable en las instituciones, en todo tipo de instituciones; este hecho se pone diariamente de manifiesto en el ámbito judicial, donde frecuentemente aparece una resistencia, contumaz en muchos supuestos, al cumplimiento de las resoluciones de los jueces y tribunales y a despecho de lo ordenado en el artículo 118 de la Constitución, lo que no es admisible en términos democráticos"[90]. Por lo tanto, estamos totalmente de acuerdo con Velasco y Saura en que ese tipo de situaciones han de ser evitadas y nos adherimos a las opiniones del Prof. Álvarez García en lo relativo a la gravedad de este tipo de comportamientos. Sin embargo, manifestamos nuestras dudas acerca de la forma de afrontar este concreto problema: la inclusión de la desobediencia en el catálogo de delitos susceptibles de ser cometidos por una persona jurídica no parece la mejor respuesta. Es más: creemos que el Derecho penal no tiene la solución, por las razones que expondremos más abajo. En nuestra opinión, ese "arsenal" que "en términos de prevención general negativa sea lo suficientemente poderoso e intimidatorio"[91] y que exige el Prof. Álvarez García para combatir la desobediencia, solamente se encuentra en el supuesto que aquí analizamos en el ámbito del Derecho administrativo sancionador.

B) *Argumentos en contra de una respuesta penal y a favor de la sanción administrativa*

A la hora de valorar las consecuencias de la posible inclusión del delito de desobediencia en el catálogo de los susceptibles de ser cometidos por personas jurídicas, nos gustaría realizar unas breves reflexiones que, creemos, hablan en contra de dar una respuesta penal y a favor de afrontar esta desobediencia desde el ámbito administrativo sancionador.

La primera consideración tiene que ver con la cuantía de la sanción y su efecto preventivo. Cuando hablamos de responsabilidad penal de la persona jurídica, resulta indiscutible el hecho de que la multa se alza como la penas por antonomasia, pues, como señala Faraldo Cabana[92], no solo es la primera que se contempla en el catálogo de penas del art. 33.7 CP, sino que, además, por regla general, es de aplicación obligatoria, frente a las demás, que resultan normalmente de aplicación potestativa.

A favor de su utilización suele esgrimirse, por lo demás, su gran efecto preventivo

[89] A quien agradezco su tiempo y sus valiosas opiniones.
[90] ÁLVAREZ GARCÍA, 2013, p. 213.
[91] Ibídem.
[92] Acerca de esta preeminencia de la pena de multa, véase FARALDO CABANA, 2015a, pp. 251-272; la misma en 2015b, pp. 3 y 4.

y su carácter óptimo, en la medida en que implica unos costes sociales mínimos en comparación con otro tipo de sanciones[93]. Ahora bien: tampoco se pueden obviar los importantes inconvenientes que surgen cuando la pena de multa es impuesta por el Derecho penal.

Como es sabido, existen dos sistemas posibles de determinación de la pena de multa: el sistema proporcional, que constituye la regla general cuando se trata de personas jurídicas, y el sistema días-multa. El sistema proporcional permite fijar la cuantía de la multa, de acuerdo con el art. 52.4 CP, en atención al beneficio obtenido o facilitado, al perjuicio causado, al valor del objeto, o a la cantidad defraudada. Pero aquí, el elemento a multiplicar resulta de muy difícil concreción. ¿Cuál es el perjuicio causado en una matanza que se podía haber evitado de haber dispuesto a tiempo de la información contenida en un móvil? ¿Cuál es el beneficio de una multinacional como Apple cuando convierte su oposición al investigador criminal en su bandera? Este problema de concreción[94] tampoco sería resuelto recurriendo al sistema de días-multa, donde, además, afrontamos otro inconveniente: la limitación existente en el Código penal para la cuantía de las multas fijadas de acuerdo con este sistema. En el sistema días-multa de la persona jurídica la cuota diaria tiene un mínimo de 30 euros y un máximo de 5.000 euros (50.4 CP). Dado que, tratándose de una persona jurídica, la extensión máxima de la pena de multa es de 5 años (art. 50.3 CP), la multa más elevada que puede imponerse es de 9.000.000 de euros (5 años x 360 días x 5.000 euros). Y a pesar de que parezca una cantidad razonable a primera vista, lo cierto es que 9.000.000 de euros constituye una cifra irrisoria para muchas multinacionales tecnológicas que no solo podrían afrontar el pago sin verse afectadas, sino que, en la práctica, ni siquiera serán ellas quienes la acaben pagando, pues en estos casos resulta frecuente que las empresas que ostentan posiciones dominantes en el mercado asuman la multa como un coste más que trasladar al cliente[95].

Por ello, en la medida en que se mantenga en nuestro país una limitación como ésta a la pena de multa[96], lo razonable parece acudir a la vía administrativa, pues allí la cuantía de las multas es mucho más elevada y se tiene también en cuenta, de manera adecuada, la reincidencia[97]. Todavía resuena el impacto de los 2.424 millones

[93] Una exposición del análisis económico de BECKNER en FARALDO CABANA, 2015a, pp. 264-269.

[94] Muchos otros problemas, de enorme trascendencia, plantea la pena de multa a la persona jurídica: los fallos de la aplicación de las leyes del mercado a una no siempre racional decisión de delinquir, la dificultad de determinar el óptimo de pena teniendo en cuenta la baja probabilidad de descubrimiento de determinados delitos, etc. Todos ellos analizados en FARALDO CABANA, 2015a, pp. 266-269.

[95] Sobre este problema puede verse ampliamente FARALDO CABANA, 2018, pp. 515 y ss. También, acerca de las dificultades de garantizar la personalidad de las penas de multa, puede verse COCA VILA, 2021, pp. 82-92. El autor califica el riesgo de pago por tercero como un "rasgo característico patológico" (p. 91) de este tipo de pena y mantiene la calificación de ese pago como constitutivo de un delito de quebrantamiento de condena (p. 92).

[96] En Inglaterra, por ejemplo, no hay límite. En España la eliminación de la limitación plantea problemas constitucionales. Véase FARALDO CABANA, 2015a, p. 263.

[97] La reincidencia constituye en Derecho Administrativo sancionador una manifestación más del principio de proporcionalidad que limita la potestad sancionadora estatal. En este sentido, por todas, la Sentencia

de euros de sanción impuesta a Google por el Tribunal de Justicia de la Unión Europea[98] por abuso de posición dominante. Como la cuantía de la multa en el ámbito administrativo es mucho más elevada, su correspondiente efecto disuasorio resulta mayor.

A la posibilidad de imponer multas de cuantía muy superior se suman otras ventajas de enorme importancia en este ámbito. No olvidemos que las exigencias que plantea una sanción penal en cuanto al respeto de una serie de garantías procesales se reducen enormemente en el procedimiento administrativo sancionador. Como recuerda Salat Paisal[99], existen diferencias en lo relativo a la asistencia letrada, a lo que puede considerarse cubierto por el derecho a la no autoincriminación, al valor de determinadas pruebas, a la presunción de inocencia, a la aplicación del *in dubio pro reo*, a los distintos efectos de las resoluciones y a los recursos que pueden interponerse frente a las mismas, entre otras. Y, además, y relacionado con lo anterior, la multa puede ser impuesta con gran celeridad en un procedimiento administrativo frente a la enorme lentitud de un proceso penal.

Todo ello también tendrá consecuencias en el plano de la prevención. Y por si todo esto fuera poco, todavía presenta el procedimiento administrativo una ventaja decisiva: en él se eliminan numerosísimos problemas jurisdiccionales que plantea la persecución de delitos cometidos por personas jurídicas que no tienen sede en España y que constituye, probablemente, el talón de Aquiles de la sanción penal en este ámbito[100]. Las incuestionables virtudes que, como vemos, posee la sanción administrativa frente a la penal nos llevan a pronunciarnos irremediablemente a favor de la primera. Por lo demás, defender en estas circunstancias la intervención del Derecho penal iría, consecuentemente, en contra de su carácter de *ultima ratio*.

Urge, por lo tanto, replantear, al menos en el ámbito europeo, una respuesta común al grave problema de la negativa de las multinacionales a colaborar con el investigador penal, especialmente si tenemos en cuenta que, debido a los avances tecnológicos de los últimos tiempos, esa relación de dependencia solamente va en aumento. Ninguno de los Ordenamientos analizados ofrece una respuesta mínimamente satisfactoria al problema. Teóricamente sería posible crear un tipo específico para sancionar

2348/2008, de 29 de abril (ECLI:ES:TS:2008:2348), recuerda que «el principio de proporcionalidad (….) tiende a adecuar la sanción, al establecer su graduación concreta dentro de los márgenes posibles, a la gravedad del hecho constitutivo de la infracción, tanto en su vertiente de antijuridicidad como de culpabilidad, ponderando en su conjunto las circunstancias objetivas y subjetivas que integran el presupuesto de hecho sancionable y, en particular, como resulta del art. 131.3 de la Ley 30/92, la intencionalidad o reiteración, la naturaleza de los perjuicios causados y la reincidencia».

[98] El fallo en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210197en.pdf.

[99] Véase SALAT PAISAL, 2021, pp. 36-40. El autor considera que las tradicionalmente calificadas como desventajas del proceso penal, o bien son inciertas, o bien juegan un papel garantista fundamental, por lo que se manifiesta, además, a favor de convertir al penal en *prima ratio* frente al Derecho administrativo sancionador (pp. 30-34 y 51-57).

[100] Acerca de los problemas procesales que hacen muy improbable la obtención de una respuesta satisfactoria, véase RODRÍGUEZ LAÍNZ, 2016, pp. 11-16.

más gravemente este tipo de desobediencia e incluir ahí la responsabilidad penal de la persona jurídica. Sin embargo, la respuesta adecuada no parece estar en manos del legislador penal, que, en el mejor de los casos, impondría una pena de multa por una cuantía irrisoria para muchas empresas de este sector, que además, con total seguridad, llegaría tarde. Por eso, la forma más adecuada de abordar este problema es a través de la respuesta rápida, realista y eficaz del Derecho administrativo sancionador.

5. **Conclusiones**

I. Las multinacionales tecnológicas desarrollan modelos de negocio reacios a cualquier actividad que suponga una mínima injerencia en la intimidad de sus clientes. En esa línea de mantener una privacidad sin fisuras, resulta frecuente que se nieguen a ayudar al investigador criminal, incluso aunque exista una orden judicial que les obligue. Especial protagonismo ha cobrado en los últimos tiempos la confrontación que mantienen la todopoderosa empresa Apple y el Gobierno de los Estados Unidos en la disputa relativa al acceso de los investigadores a los teléfonos móviles encriptados. Este debate no es ajeno a nuestro país: la UCO, probablemente previendo la respuesta negativa de Apple, recabó la ayuda de *Cellebrite* para tratar de acceder a la información contenida en el teléfono móvil de la desaparecida Diana Quer, y en el caso Dina Bousselham el juez instructor solicitó la ayuda de la empresa Samsung para acceder a la tarjeta de memoria, advirtiendo al Director del Departamento legal que la negativa de la empresa podía dar lugar a que él incurriera en un delito de desobediencia.

II. El Convenio de Budapest fue consciente de esa relación de dependencia y exhortó a los Estados a regular deberes de colaboración para el sector privado. Cada Estado europeo ha establecido al respecto una regulación propia, destacando particularmente la de Francia que, desde el año 2001, ha tipificado como delito la mera negativa a proporcionar convención secreta de descifrado de un medio criptológico, y desde 2004, ha incluido como agravante la comisión de un delito utilizando medios criptológicos. En Alemania, por su parte, el § 100j StPO permite solicitar esta colaboración a las empresas de telecomunicaciones, y su incumplimiento da lugar a la imposición de las mismas medidas coercitivas que en el caso de la negativa injustificada a testificar o a prestar juramento. En Italia, desde el año 2008, el art. 256 CPPit, dedicado al deber de exhibición y secreto, incluye también el deber de proporcionar los datos y programas informáticos, y sanciona el incumplimiento a través del delito de desobediencia genérica del art. 650 CPit., constituyendo el incumplimiento una contravención, susceptible *oblazione* facultativa. En España, por último, junto a los regulados en determinadas normas administrativas, la LECrim establece

dentro de las medidas de investigación tecnológica una serie de deberes de colaboración y se remite al delito de desobediencia para castigar su incumplimiento (588 ter e. 3; 588 sexies c. 5; 588 septies b. 4 y 588 octies LECrim). Las referencias a este delito solamente se mantienen en el Anteproyecto de LECrim de 2020 en lo relativo al registro de dispositivos de almacenamiento masivo, pero han sido eliminadas tanto en la intervención de las comunicaciones, como en el registro remoto y en la orden de conservación de la información. No disponemos, a diferencia de Francia, de ninguna agravante genérica que sancione la comisión por medio de un sistema informático. No obstante, en la medida en que se mantenga el fundamento de las tradicionales agravantes del art. 22.2 CP, convendría repensar su posible introducción en una futura reforma.

III. No parece admisible dejar sin respuesta la negativa a colaborar en la investigación criminal, pues resulta de todo punto inaceptable que los intereses económicos de las empresas tecnológicas y un ilimitado derecho a la intimidad cuya protección falsa e interesadamente enarbolan, generen un espacio de impunidad en el que al investigador criminal le sea vetado el acceso. Cuestión distinta es cómo ha de abordarse este incumplimiento. Si se opta por una respuesta penal, resulta correcta la sanción por desobediencia, ya sea mediante la aplicación del tipo tradicional de desobediencia genérica, ya sea creando uno específico, como se ha hecho en Francia. En todo caso, con el objeto de poder sancionar el incumplimiento de las empresas tecnológicas habría que incorporar la desobediencia genérica -como propone algún autor- o el delito específico de nuevo cuño resultante al catálogo de aquellos que pueden ser cometidos por personas jurídicas.

IV. Consideramos, sin embargo, que la respuesta al incumplimiento de los deberes de colaboración de las multinacionales tecnológicas no ha de provenir del Derecho penal, pues éste parece incapaz de dar una respuesta satisfactoria al problema del incumplimiento desde la óptica de la prevención general negativa. Diversas razones hablan en contra de un abordaje penal del problema y a favor del recurso en esta materia a las sanciones pecuniarias del Derecho administrativo sancionador que, además, otorga relevancia al fenómeno de la reincidencia: se evitan los problemas que plantea la imposición de la pena de multa por parte del Derecho penal tanto en lo que respecta a los criterios para su determinación, como en lo relativo a los límites de su cuantía; se consigue una celeridad en la imposición de las sanciones inalcanzable para el Derecho penal y, lo que es más importante, se logran evitar múltiples problemas de jurisdicción que el recurso al castigo penal plantea. El adecuado tratamiento de la negativa a colaborar se encuentra en otra rama del Ordenamiento, por lo que mantener una sanción penal en este ámbito vulnera el principio de *ultima ratio*. En todo caso, en estos tiempos en los que parece aproximarse la elaboración de un nuevo Ciberconvenio sustitutivo del de Budapest, y teniendo en cuenta que ninguno de los Ordenamientos analizados ofrece una respuesta satisfactoria a esta cuestión, resulta

conveniente plantear la elaboración de una normativa común en el ámbito europeo para dotar a un problema creciente y grave de una respuesta única que, si proviene del Derecho administrativo sancionador, será, además, rápida y eficaz.

Bibliografía

ABEL SOUTO, M. (2021), "Algunas discordancias legislativas sobre la responsabilidad penal de las personas jurídicas en el Código penal español", *Revista General de Derecho penal,* n. 35, pp. 1-62.

ALEO, S. (2008), *Il sistema penale*, Milán.

ALONSO RIMO, A. (2020), "¿Desobediencia a la autoridad o a la ley?: Reflexiones sobre el objeto de tutela del delito y la infracción administrativa de desobediencia (a propósito del debate sobre su aplicación durante la pandemia de COVID-19)", en Alapont (coord.); González Cussac (dir.): *Estudios jurídicos en memoria de la Profesora Doctora Elena Górriz Royo*, pp. 85-110.

ÁLVAREZ GARCÍA, F. J. (2007), "Sobre quebrantamiento de condena, desobediencias, impago de pensiones, falta de comparecencia a comisiones de investigación y citaciones judiciales", en *Revista de Derecho penal y Criminología*, n. 19, pp. 9-38.

ÁLVAREZ GARCÍA, F. J. (2013), "Las desobediencias en Derecho Penal*",* en *Eunomía, Revista en Cultura de la Legalidad*, n. 4, pp. 208-215.

AUDIBERT, M. (2020), "Code de déverrouillage d'un téléphone portable", en *Veille juridique*, n. 90, pp. 24-36.

BAFFA, G. (2020), "Grovigli normativi ed «efficientismo» punitivo nella risposta sanzionatoria all'emergenza Covid-19. Una «guerra» combattuta con le armi della decretazione d'urgenza", en Massaro (coord..): *Connessioni di Diritto penale*, Roma, pp. 15-52.

BOCANEGRA MÁRQUEZ, J. (2022), "La inobservancia de las limitaciones de la libertad circulatoria en los estados de alarma declarados durante la pandemia por COVID-19: ¿delito, infracción administrativa o acto sin consecuencias jurídicas?", en *Revista Electrónica de Ciencia Penal y Criminología*, n. 24-17, pp. 1-31.

BONIS, É.; PELTIER, V. (2018), "Chronique de droit pénal et de procédure pénale", en *Titre VII*, n. 1, pp. 72-80.

BONTEMPELLI, M. (2015), "Il procedimento di oblazione", en Spangher, Marandola, Garuti, Kalb (dirs.): *Procedura penale: teoría e pratica del proceso*, Milán, pp. 473-548.

CANZIO, G.; LUPARIA, L. (2018), *Prova scientifica e processo penale*, Milán.

CARDENAL MONTRAVETA, S. (2007), "Los delitos relacionados con la seguridad del tráfico en el derecho comparado", en *Indret*, *Revista para el análisis del Derecho*, pp. 1-33.

CARDENAL MONTRAVETA, S. (2015), "¿Eficacia preventiva general intimidatoria de la pena?", en *Revista Electrónica de Ciencia Penal y Criminología,* n. 17-18, pp. 1-44.

CARUSO FONTÁN, M. V. (2019), "Cuando los juegos se vuelven peligrosos. La criminalidad en los espacios virtuales multijugador", en *La Ley penal*, n. 141, pp. 1-28.

CERDA GUZMÁN, C.; GUGLIELMI, G. J. (2021), *Las Sentencias básicas del Consejo Constitucional francés*, Madrid.

COCA VILA, I. (2021), "La pena de multa en serio. Reflexiones sobre su dimensión y aseguramiento aflictivos a través del delito de quebrantamiento de condena (art. 468 CP)", en *Indret*, *Revista para el análisis del Derecho*, pp. 69-99.

COCO, P. (2021), "Brevi reflesioni sull'illecito contravencionale", en Catenacci; D'Ascola; Rampioni (coords.): *Studi in onore di Antonio Fiorella*, Roma, pp. 11-142.

DAVARA FERNÁNDEZ DE MARCOS, E.; DAVARA FERNÁNDEZ DE MARCOS, L. (2017), en Davara Rodríguez (coord.): *Delitos Informáticos*, Pamplona.

DE COMBLES DE NAYVES, P. (2019), "Le code de déverrouillage d'un télephone n'est pas une convention de déchiffrement", *Dalloz AJ penal*, pp. 439-443.

DERIEUX, E. (2018), "Déchiffrement forcé d'un moyen de cryptologie", en *Revue européenne des médias et du númerique*, n. 46-47, pp. 1-4.

DOPICO GÓMEZ-ALLER, J. (2011), "Las circunstancias agravantes de abuso de superioridad, disfraz y aprovechamiento de otras circunstancias. Estudio jurisprudencial", en *La Ley penal*, n. 83, pp. 87-94.

ESCUDERO GARCÍA-CALDERÓN, B. (2021), "El investigado o encausado, el abogado y el pariente como sujetos excepcionados del deber de colaborar en la obtención de la prueba digital", en *Revista General de Derecho Penal*, n. 36, pp. 1-44.

ESCUDERO GARCÍA-CALDERÓN, B., "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", en *Anuario de Derecho Penal y Ciencias Penales*, en prensa.

FARALDO CABANA, P. (2015a), "Acerca de la idoneidad de la sanción pecuniaria para personas jurídicas. Una reflexión de Derecho español con apuntes de Derecho italiano", en *Economía y Derecho penal en Europa: una comparación entre las experiencias italiana y española, Actas del Congreso hispano-italiano de Derecho penal económico (Università degli Studi di Milano, Milano, 29-30 de mayo de 2014)*, pp. 251-272.

FARALDO CABANA, P. (2015b), "La obligatoria modulación de las multas penales impuestas a la persona jurídica y a la persona física", en *La Ley Penal*, n. 115, pp. 1-11.

FARALDO CABANA, P. (2018), "La transmisibilidad de la pena de multa en las modificaciones estructurales. Sobre la aplicación del principio de personalidad de las penas a las personas jurídicas", en Morales Prats; Tamarit Sumalla; García Albero (coords.): *Represión penal y estado de derecho: Homenaje al Profesor Gonzalo Quintero Olivares,* Pamplona, pp. 515-529.

GARCÍA MENÉNDEZ, M. (2021), ¿Hacia un nuevo Convenio de Budapest sobre la ciberdelincuencia?, en *Actualidad Jurídica Aranzadi,* Sección opinión, n. 979.

GARCÍA PLANAS, G. (1999-2000), "Nociones acerca de la agravante de disfraz en la jurisprudencia del Tribunal Supremo", en *Estudios penales y Criminológicos*, n. 22, pp. 33-54.

GRIMM, M. P. (2021), *Das Insiderhandelsverbot zwischen Rechtstheorie und Rechtspraxis: Chancen und Risiken eines Einsatzes von Big Data und Künstlicher Intelligenz in der Rechtsdurchsetzung*, Baden-Baden.

KELLER, C.; BRAUN, F. (2019), *Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen*, 3ª ed., Stuttgart, Múnich, Hannover, Berlín, Weimar, Dresden.

LÓPEZ BARJA DE QUIROGA, J. (2014), *Tratado de Derecho Procesal Penal*, Tomo II, 6ª ed., Navarra.

LORENTE VELASCO, S. M. (2010), *Delitos de atentado contra la autoridad, sus agentes y los funcionarios públicos y de resistencia y desobediencia*, Madrid.

MARCHENA GÓMEZ, M. (2001), "Perseguibilidad de los delitos en Internet", en Davara Rodríguez, (coord.): *JIS'2000, III Jornadas sobre informática y sociedad*, Madrid, pp. 159-186.

MARCHENA GÓMEZ, M.; GONZÁLEZ-CUÉLLAR SERRANO, N. (2015), *La Reforma de la Ley de Enjuiciamiento Criminal de 2015*, Madrid.

PAOLETTI, A. (2020), *La ricerca della prova penale nell'era delle nuove tecnologie informative*, Milán.
PELLIZZONE, I. (2015), *Profili constituzionali della reserva di legge in materia penale*, Milán.
QUINTERO OLIVARES, G. (2021), "La revisión de los delitos de desobediencia", en *Revista Aranzadi Doctrinal*, n. 1, pp. 1-18.
RODRÍGUEZ LAINZ, J. L. (2016), "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?", en *Diario La Ley*, n. 8729, pp. 1-16.
ROUSSEL, B. (2020), *Les investigations numériques en procédure pénale*, Universidad de Burdeos.
RUBIO ALAMILLO, J. (2015), "La informática en la reforma de la Ley de Enjuiciamiento Criminal", en *Diario La Ley*, n. 8662, pp. 1-11.
SALAT PAISAL, M. (2019), "El Derecho penal como prima ratio. La inadecuación del derecho administrativo sancionador y la necesidad de buscar soluciones en el seno del Derecho penal", en *Revista General de Derecho Administrativo*, n. 51, pp. 1-57.
SANDOVAL REYES, S. (2020), "Las medidas coercitivas alemanas (en sentido restringido) como equivalentes a las diligencias de investigación en el procedimiento penal", en *Revista de Ciencias Sociales*, n. 76, pp. 145-168.
VELASCO NÚÑEZ, E. (2010), *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid.
VELASCO NÚÑEZ, E. (2016), *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Madrid.
VELASCO NÚÑEZ, E.; SAURA ALBERDI, B. (2016), *Cuestiones Prácticas sobre Responsabilidad penal de la persona jurídica y Compliance*, Cirzur Menor (Navarra).
VOSS, T; MÖLLER-BERTRAM, R. (2022), "Kann der Gesetzgeber das Ziel- Schaffung einer intensiveren un effektiveren Strafvervolgung con Rechtextremismus uns Hasskriminalität- mit dem Gesetzentwurf BT Drs 19/17741 erreichen", en Stember (edit.): *Neue Erkenntnisse uns Ansätze im Polizei-, Verwaltungs- und öffentlichen Finanzmanagement*, Baden-Baden, pp. 307-330.