SECONDA EDIZIONE DEL SEMINARIO INTERNAZIONALE DI DIRITTO COMPARATO
«DIRITTO E NUOVE TECNOLOGIE TRA COMPARAZIONE E INTERDISCIPLINARITÀ»
- IN MEMORIA DEL PROF. PAOLO CARROZZA -

VIDA PRIVADA *VERSUS* SEGURIDAD PÚBLICA: EN BUSCA DE UNA SOLUCIÓN PONDERADA AL CIFRADO FUERTE DE COMUNICACIONES

JUAN OCÓN GARCÍA

SUMARIO: 1. Introducción. – 2. El cifrado extremo a extremo en la encrucijada entre libertad y seguridad. – 3. Criptografía y derechos fundamentales. – 4. Soluciones de regulación. – 4.1. Establecimiento de condiciones de eficacia prospectiva. – 4.2. Imposición de deberes en investigaciones en marcha. – 5. Soluciones de intervención. – 6. Conclusiones.

1. *Introducción*

La criptografía, que podemos definir como el arte y la ciencia de la escritura secreta, permite que un texto —texto claro— se convierta en un criptograma —texto cifrado— mediante la aplicación de una serie de operaciones —algoritmo de cifrado—.

El elemento más importante es la clave criptográfica, esto es, la información que aplicada al algoritmo permite al emisor cifrar el texto claro y al destinatario descifrar el criptograma. En los esquemas de cifrado extremo a extremo, habitualmente incorporados en la actualidad a las plataformas comunicativas más generalmente utilizadas, las claves de cifrado se almacenan únicamente en los dispositivos de los comunicantes, lo que dificulta su desactivación en aquellos casos que resulta necesario y constitucionalmente legítimo.

El cifrado refuerza técnicamente la eficacia de algunos derechos fundamentales, pero a su vez obstaculiza el normal desarrollo de las competencias de los Estados para

garantizar la seguridad pública, exigiendo por ello una solución ponderada[1]. El presente trabajo analiza algunas de esas posibles soluciones.

2. *El cifrado extremo a extremo en la encrucijada entre libertad y seguridad*

El intercambio de información entre personas físicamente distantes ha sido históricamente dotado de garantías frente a descubrimientos indeseados de terceros. Sistemas de codificación como la escítala espartana o la cifra César constituyen los primeros ejemplos del uso de criptografía en la época clásica[2].

Desde entonces, el avance de las técnicas criptográficas no se ha detenido. Su evolución estuvo marcada, primero, por la mecanización —cuyo ejemplo más notorio es la máquina Enigma— y, posteriormente y con mayor incidencia, por el auge de la informática, permitiendo la generación de claves más seguras, la estandarización de algoritmos y el desarrollo de criptosistemas asimétricos o de clave pública.

El nacimiento y desarrollo de Internet ha ido generando cada vez más relaciones complejas de carácter global en las que los flujos de información se transmiten en línea, demandando una creciente protección de las transacciones informáticas de datos. Del mismo modo, la red ha ido transformando las comunicaciones, cada vez más sencillas, veloces y accesibles a la mayoría de la población. Pero también ha ido ofreciendo crecientes posibilidades de interceptar procesos comunicativos y, por ende, un mayor grado de exposición a acciones de vigilancia masiva o de retención generalizada de datos de tráfico.

Como reacción a esta situación de sobrevigilancia, las organizaciones públicas y privadas, y cada vez más los ciudadanos, comienzan a buscar protección adicional para mantener reservado el contenido de sus comunicaciones más allá de la mera protección jurídica[3]. De esta forma, la criptografía se desgaja de su tradicional uso militar o político hasta generalizarse también entre particulares.

En la actualidad el cifrado de comunicaciones interpersonales está completamente generalizado y accesible: millones de personas intercambian diariamente millones de mensajes encriptados sin ser, en muchos casos, conscientes de ello. La incorporación por defecto de técnicas de cifrado extremo a extremo a plataformas comunicativas de uso generalizado —WhatsApp, Skype, Telegram, …— supone que una buena parte de las

[1] Para una visión global de la relación que la criptografía mantiene con el Derecho, puede acudirse a G. ZICCARDI, *Crittografia e diritto: crittografia, utilizzo e disciplina giuridica, documento informatico e firma digitale, segretezza delle informazioni e sorveglianza globale*, Torino, 2003.

[2] *Vid*. S. SINGH, *Los códigos secretos. El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de Internet*, Barcelona, 2000, 21 y ss.

[3] Hurwitz habla de un «efecto de compensación»: «While law enforcement is losing access to much of the investigative information that it has traditionally sought, it (along with non-law enforcement entities) is also gaining access to troves of new information». J. HURWITZ, *Encryption Congress Mod (Apple + CALEA)*, en *Harvard Journal of Law & Technology*, vol. 30, 2/2017, 400. Véase también D. ÁLVAREZ VALENZUELA, *Algunos aspectos jurídicos del cifrado de comunicaciones*, en *Derecho PUCP*, 83/2019, 243.

comunicaciones intercambiadas cada día resulten ilegibles por terceros ajenos mientras transitan por la red.

En los esquemas de cifrado de este tipo las claves criptográficas se almacenan únicamente en los dispositivos de los usuarios, de modo que solo remitente y receptor pueden descifrar el mensaje intercambiado. Los operadores de servicios de comunicaciones no pueden, por tanto, cumplir eficazmente las órdenes de intervención para las que se requiere de su asistencia[4].

El uso extendido de cifrado *end-to-end* ha suscitado la preocupación de los Estados en tanto que esta tecnología disminuye su eficacia en la prevención e investigación criminal. Surgen así diferentes propuestas de regulación que abarcan desde su absoluta prohibición hasta su total libertad, pasando por soluciones intermedias consistentes principalmente en la imposición de deberes a distintos sujetos.

En los últimos años han sido habituales las declaraciones, informes y recomendaciones de organismos internacionales preocupados por las dificultades que genera para las competencias de los Estados el uso generalizado de sistemas de cifrado fuerte.

Este es el sentido de la *International Statement: End-to-end encryption and public safety*, firmada en octubre de 2020 por India, Japón y los Estados que componen la alianza de inteligencia conocida como *Five Eyes* (Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda) cuya propuesta principal se orienta a garantizar, desde el diseño y en colaboración con las compañías tecnológicas, el acceso a datos cifrados[5].

También de la Resolución del Consejo de la Unión Europea de noviembre de 2020 «La seguridad mediante el cifrado y a pesar del cifrado», que apuesta por el desarrollo y utilización de cifrado fuerte, pero sin renunciar a aplicar soluciones técnicas que permitan a las autoridades ejercer sus competencias de investigación[6].

Se trata, en definitiva, de hallar una solución ponderada a un escenario de alta tensión del binomio libertad-seguridad.

3. *Criptografía y derechos fundamentales*

Las distintas soluciones de regulación sobre el desarrollo y utilización de sistemas de cifrado de comunicaciones pueden implicar a diversos derechos fundamentales generalmente reconocidos en los catálogos de derechos de las constituciones occidentales.

El desarrollo y difusión de algoritmos de cifrado, en cuanto expresión de un lenguaje específico, puede ser considerado una forma de libertad de expresión o, más

[4] Véase, A. ETZIONI, *Ultimate Encryption*, en *South Carolina Law Review*, vol. 67, 3/2015; y J.L. MORENO FONTELA, *Servicios cifrados de extremo a extremo e investigación penal bajo derecho español*, en J. VALLS PRIETO (coord.), *Retos jurídicos por la sociedad digital*, Cizur Menor, 2018, 269-299.

[5] Disponible en: https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

[6] Disponible en: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/es/pdf

concretamente, encontrar amparo en el derecho a la libertad de creación científica reconocido por algunos textos constitucionales[7].

Por su parte, la utilización de cifrado involucra a aquellos derechos que se dirigen a garantizar espacios de inmunidad en la vida privada de los ciudadanos. El mero recurso al cifrado advierte una pretensión del usuario de reservar la información así protegida del conocimiento de los demás, lo que se identifica con el objeto del derecho fundamental a la intimidad. Del mismo modo, supone una garantía adicional, en algunos casos normativamente recomendada[8], de los datos de carácter personal objeto de transmisión. Y, sobre todo, proporciona un refuerzo de carácter técnico que se adosa a la garantía jurídico-formal dispensada por el derecho fundamental al secreto de las comunicaciones. Además, los esquemas de cifrado extremo a extremo refuerzan el secreto precisamente en la fase más vulnerable del proceso comunicativo: aquella en que su control se sustrae a los comunicantes y pasa a depender del prestador del servicio[9].

En todos estos casos, sin embargo, la criptografía guarda con los derechos fundamentales referidos una relación de instrumentalidad en la que claramente puede diferenciarse derecho protegido y artificio tecnológico para su preservación, pero en ningún caso el uso de la criptografía forma parte de su contenido esencial. No es posible identificar un derecho constitucionalmente garantizado a la utilización de sistemas de cifrado de comunicaciones.

La decisión sobre el modo de regular la criptografía es, por tanto, de carácter político o de oportunidad, pero no por ello incondicionada. En la medida en que el uso de la criptografía puede incidir, como garantía material de carácter tecnológico, en la efectividad de diversos derechos fundamentales deberá tenerse en cuenta su dimensión objetiva.

Los derechos fundamentales, en tanto que expresión de un sistema de valores, además de operar como derechos subjetivos actúan como directrices constitucionales y

---

[7] *Vid.* artículos 20.1.b) de la Constitución Española; 5.3 de la Constitución Alemana y 13 de la Carta de Derechos Fundamentales de la Unión Europea. Respecto a la protección dispensada por la Primera Enmienda a la Constitución estadounidense resulta obligada la cita al asunto *Bernstein v. United States*, en el que el tribunal concluyó: «that encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive for First Amendment purposes, and thus is entitled to the protections of the prior restraint doctrine», *United States Court of Appeals, Ninth Circuit. No. 97-16686 (May 06, 1999)*. Sobre la protección del código informático como *discurso* o *conducta* en el objeto de la Primera Enmienda, véase T. NGUYEN, *Cryptography, export controls, and The First Amendment in Bernstein v. United States Department of State*, en *Harvard Journal of Law & Technology*, vol. 10, 3/1997, 667-682; R. POST, *Encryption Source Code and the First Amendment*, en *Berkeley Technology Law Journal*, 15/2000, 713-723 y D. MCCLURE, *First Amendment Freedoms and the Encryption Export Battle: Deciphering the Importance of Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999)*, en *Nebraska Law Review*, vol. 79, 2/200, 465-484.

[8] *Vid.* art. 32.1.a) 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.

[9] «The underlying rationale to warrant such protection is that communicants entrust communication to an intermediary, thus losing control in relation to the intermediary or third parties»; cfr. F.J. ZUIDERVEEN BORGESIUS and W. STEENBRUGGEN, *The right to communications confidentiality in Europe: protecting privacy, freedom of expression, and trust*, en *Theoretical Inquiries in Law*, vol. 20, 1/2019, 299.

reglas de actuación legislativa, obligando a los poderes públicos a contribuir a su efectividad[10].

En la medida en que el recurso a la criptografía puede proporcionar una mayor efectividad de los derechos descritos, su total prohibición resulta contraria a las obligaciones positivas que para los Estados derivan de la dimensión objetiva de los derechos y, por tanto, no puede ser una opción constitucionalmente atendible.

Sin embargo, los derechos fundamentales no tienen carácter absoluto, y su limitación resulta en ocasiones necesaria para garantizar otros bienes jurídicos o derechos igualmente relevantes. Por su parte, la criptografía mantiene con estos derechos una relación inevitablemente ambivalente, pues si bien refuerza materialmente su objeto, obstaculiza su legítima desactivación. Estamos pues ante una tecnología de doble uso: sirve al derecho al tiempo que lo amenaza, al disminuir sensiblemente la capacidad de los poderes públicos de alcanzar los objetivos legítimos para cuya consecución se habilita constitucionalmente la limitación de los derechos considerados.

A la hora de regular este tipo de tecnologías deben ponderarse sus riesgos y beneficios. Lichlyter propone una rúbrica basada en tres categorías de amenazas y beneficios de las tecnologías de doble uso, concluyendo que la criptografía supone una amenaza de daño de tipo dos; pero ofrece beneficios de las categorías A y C[11].

El cifrado puede ser utilizado en ocasiones para obstaculizar la investigación criminal, pero tiene sobre todo una gran capacidad para evitar la comisión de determinados delitos, como el fraude en operaciones bancarias a través de la red o el espionaje industrial.

Resulta necesario, por tanto, adoptar un sistema que permita el uso de técnicas de cifrado y, al mismo tiempo, garantice el normal desarrollo de las actividades estatales dirigidas a salvaguardar la seguridad.

Descartada su prohibición, es posible sistematizar en dos grandes grupos las potenciales soluciones: por un lado, aquellas que consisten en el establecimiento de una regulación previa y de carácter general imponiendo bien determinadas características a los sistemas de cifrado permitidos, bien determinados deberes a sus creadores o usuarios; por otro, aquellas que, permitiendo el libre desarrollo y utilización del cifrado, operan sobre casos concretos persiguiendo su desactivación mediante técnicas diversas.

[10] Una visión histórica de la doctrina de la doble dimensión de los derechos fundamentales y su incidencia en diversos ordenamientos puede hallarse en A. DI MARTINO, *La doppia dimensione dei diritti fondamentali*, en *Rivista del Gruppo di Pisa*, 2/2016, 1-63.

[11] Los peligros de tipo 1 se corresponden con los daños directos, los de tipo 2 con aquellos causados dentro un único curso de conducta (la destrucción de pruebas de la comisión de un delito o la obstrucción a su investigación) y los de tipo 3 con los daños provenientes de una acción separada, pero facilitada por el uso de la tecnología en cuestión. Por su parte, los beneficios de tipo A se identifican con las mejoras relevantes para el ejercicio de derechos constitucional, los de tipo B con los beneficios para la salud o la seguridad y los de tipo C con la eficiencia de recursos o las preferencias personales. L. LICHLYTER, *Encryption, guns, and paper shredders: analogical reasoning with physically dangerous technologies*, en *Harvard Journal of Law & Technology*, vol. 31, 1/2017, 259-273.

4. *Soluciones de regulación*

Nos referimos en este apartado a aquellas propuestas que consisten en establecer, con carácter general, el cumplimiento de determinados requisitos para el desarrollo o utilización de sistemas de cifrado. Dentro de esta categoría podemos diferenciar entre aquellas propuestas que consisten en la imposición de condiciones que deben cumplirse con independencia de la existencia de una concreta investigación y que tendrán, en su caso, una potencial eficacia en el futuro, y aquellas otras que imponen condiciones que, aunque previstas normativamente con carácter previo y general, solo se activan con ocasión de una concreta investigación ya en marcha.

4.1. *Establecimiento de condiciones de eficacia prospectiva*

La primera de las soluciones de este tipo consiste en autorizar exclusivamente el desarrollo, comercialización y utilización de sistemas criptográficos que permitan a las autoridades acceder a la información codificada, lo que puede lograrse bien mediante el debilitamiento del algoritmo de cifrado, bien mediante un sistema de claves en custodia. Ambos casos, sin embargo, plantean dificultades insalvables.

En primer lugar, resulta extremadamente complejo técnicamente implementar sistemas de cifrado debilitados sin que ello suponga su inutilización práctica. La misma dificultad se evidencia en los sistemas de custodia de claves, que exigen el desarrollo de criptosistemas de múltiples partes y, por ello, expuestos a vulnerabilidades de seguridad[12].

Los sistemas de depósito de claves —*key escrow*— consisten en la imposición a usuarios y fabricantes de tecnología de encriptación de la obligación de depositar las claves en ciertos organismos de confianza (*Trusted Trird Partys*, TTP´s), como encargados de su custodia y cesión a las autoridades en caso de que sea necesario acceder a la información cifrada. Por su parte, en los sistemas de recuperación de claves —*key recovery*— es el propio sistema de cifrado el que permite a los organismos de confianza, una vez autorizados, reconstruir la clave a partir de vulnerabilidades en el sistema[13].

En ambos casos se consigue la finalidad pretendida: se habilita el uso de cifrado a la vez que se posibilita el acceso a los contenidos transmitidos en una eventual investigación penal. Sin embargo, una vez que la clave ha sido utilizada, previa cesión o

[12] J. HURWITZ, *Encryption Congress*, cit., 413-414.

[13] E. FRYE y R.V. SABETT, *Key recovery in a public key infrastructure*, en *Jurimetrics*, vol. 38, 3/1998, 485-496. El denominado Clipper Chip, promovido por la administración Clinton entre 1993 y 1998, constituye ejemplo más conocido de este tipo de propuestas. Sobre el ejemplo estadounidense, S. ANDREWS, *Who Holds the Key? A Comparative Study of US and European Encryption Policies*, en *The Journal of Information, Law and Technology*, 2/2000 y S. BRADY, *Keeping secrets: a constitutional examination of encryption regulation in the United States and India*, en *Indiana International & Comparative Law Review*, vol. 22, 2/2012, 329 y ss.

reconstrucción, todas las comunicaciones encriptadas con dicha clave son potencialmente descifrables[14].

Además de las dificultades técnicas aludidas, las principales críticas a los regímenes de custodia de claves se han centrado en la escasa eficacia que poseen frente a la delincuencia grave, dada la facilidad para eludir estos sistemas modificando el *software* de cifrado o adquiriendo sistemas alternativos, y en la posibilidad de que las puertas traseras habilitadas con las claves depositadas se conviertan en objetivos para los delincuentes[15]. Pero, sobre todo, por la incidencia que un sistema de este tipo puede generar en la confianza de los ciudadanos, creando una atmosfera de sospecha constante[16].

La segunda posibilidad que podemos incluir en este apartado consiste en el establecimiento de requisitos de capacidad a los prestadores de servicios y productos de tecnologías de la información. Se trata de imponer normativamente la necesidad de poseer la capacidad de facilitar a las autoridades la información descifrada en aquellos casos constitucionalmente permitidos. Una obligación que, para ser eficaz en el escenario convergente actual, debiera tener como destinatarios no solo a los tradicionalmente sujetos a regulaciones de este tipo —los operadores de servicios de comunicaciones—, sino también a prestadores de servicios de la sociedad de la información y fabricantes de dispositivos[17].

Pueden imputarse a esta solución las mismas críticas que a la anteriormente descrita: no es posible asegurar su efectividad en la medida en que es sencillo sortear la norma acudiendo a software de cifrado extranjero o de código abierto[18]. Podría ser útil, no obstante, respecto de aquellos servicios que incorporan cifrado de forma predeterminada y son generalmente utilizados (iPhone, WhatsApp), pudiendo actuar como «cuellos de botella»[19].

No obstante, resultaría una medida ineficaz frente a la delincuencia grave, que es precisamente aquella a la que se alude al tratar de justificar la necesidad de imponer regulaciones restrictivas al cifrado.

Se trata además de una solución frontalmente opuesta a la tendencia actual del mercado de tecnologías de la información y comunicación, que transita progresivamente hacía la implantación de cifrado *end-to-end* caracterizado precisamente por la

[14] *Vid.* Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, 8 de octubre de 1997, «Garantizar la seguridad y la confianza en la comunicación electrónica. Hacia un marco europeo para la firma digital y el cifrado», anexo III.

[15] «Pretender afianzar la lucha contra el crimen mediante la imposición de normas jurídicas en la utilización del cifrado, cuando el adversario se caracteriza precisamente por su desprecio hacia ellas, resulta al menos ilusorio»; cfr. B.A. GONZÁLEZ NAVARRO, *Criptología y libertades públicas*, en *Cuadernos de Derecho Judicial. Internet y derecho penal*, 10/2011, 208.

[16] La obligación de depositar las claves de custodia ha sido gráficamente comparada con una hipotética obligación de coser copias de látex de las huellas dactilares en la punta de los dedos de los guantes. R.L. RIVEST, *The Case against Regulating Encryption Technology*, en *Scientific American*, 279/1998, 116-117.

[17] *Vid*. J. HURWITZ, *Encryption Congress*, cit., 419-420.

[18] O.S. KEER y B. SCHNEIER, *Encryption Workarounds*, en *Georgetown Law Journal*, 106/2018, 1013.

[19] J. HURWITZ, *Encryption Congress*, cit., 419.

incapacidad del prestador del servicio o fabricante del dispositivo para conocer las claves de cifrado.

4.2. *Imposición de deberes en investigaciones en marcha*

El segundo grupo de soluciones de regulación consiste en la imposición de deberes a distintos sujetos con el objetivo de hacer posible el acceso a información protegida por sistemas de cifrado en investigaciones en curso.

La primera posibilidad, normativamente extendida, consiste en la imposición de deberes de asistencia para descifrar a desarrolladores de criptografía y prestadores de productos o servicios que incorporan sistemas de cifrado[20].

Esta solución puede generar conflictos directos entre los intereses de las autoridades y de la parte obligada, que se ve forzada a debilitar los productos que ella misma diseña[21]. Los requisitos de asistencia pueden suponer una amenaza frontal a las propias políticas comerciales de las empresas del sector tecnológico, en buena medida orientadas a ofrecer el máximo nivel posible de seguridad como pilar estratégico de su oferta. El conocido caso del atentado de San Bernardino constituye un ejemplo notable de este problema[22].

Además, las normas que prevén este tipo de deberes acostumbran a incorporar requisitos de proporcionalidad, evitando que la asistencia consista en una carga irrazonable para la parte obligada. Una previsión que, como acertadamente han observado Kerr y Schneider, puede frustrar la eficacia de esta solución: los sistemas de cifrado pueden ser diseñados en su origen para convertir las solicitudes de asistencia técnica futuras en desproporcionadas[23].

No obstante, si bien la imposición de deberes de colaboración a sujetos técnicamente solventes no puede constituir una solución eficaz en exclusividad, sí puede resultar de utilidad, como veremos, en combinación con otras técnicas de acceso a comunicaciones cifradas.

La última de las posibles soluciones de este tipo consiste en imponer la obligación de aportar las claves de cifrado a cualquier persona que las conozca, incluido el propio

[20] Así, por ejemplo, en la *Communications Assistance for Law Enforcement Act* estadounidense o los artículos 588 ter.e y septies.b de la Ley de Enjuiciamiento Criminal española.

[21] O.S. KEER y B. SCHNEIER, *Encryption Workarounds*, cit., 1016.

[22] *Vid.* A. ETZIONI, *Apple: Good Business, Poor Citizen?*, en *Journal of Business Ethics*, 151/2018, 1-11.

[23] O.S. KEER y B. SCHNEIER, *Encryption Workarounds*, cit., 1017-1018. De esta realidad, para el caso de los teléfonos Apple, da cuenta Hurwitz: «Apple has designed its modern iPhones to have a secret unique device ID (so secret, in fact, that not even Apple knows or can determine what it is) contained on a physical chip in the phone. This device ID is used as part of the de-vice's encryption key — you need it in order to decrypt the contents of the phone. But Apple designed the iPhone such that the device ID is inaccessible to anyone. The iPhone's internal circuitry can use the de-vice ID when calculating encryption keys — but there is no way for it to share the device ID itself. In other words, Apple has designed its recent iPhones in a way that makes it technologically impossible for anyone — Apple or the user of any iPhone — to provide all of the information necessary to decrypt the information on the device»; J. HURWITZ, *Encryption Congress*, cit., 421.

titular de la información protegida. Obligación que suele acompañarse de la creación de un tipo penal dirigido a castigar su incumplimiento[24].

Dos son las principales criticas que se pueden oponer a esta propuesta. En primer lugar, cuando el sujeto obligado es el propio investigado, esta previsión puede resultar contraria al derecho fundamental a la presunción de inocencia[25]. En segundo lugar, la medida se tornará ineficaz en aquellos casos en que la sanción prevista para el delito investigado sea mayor que la dispuesta para la negativa a aportar las claves de cifrado, permitiendo al sujeto investigado asumir la menor condena, lo que disminuye en consecuencia la eficacia de la medida precisamente en la lucha contra la delincuencia grave.

5. *Soluciones de intervención*

Los grandes inconvenientes que presentan las soluciones de regulación nos inclinan a considerar más apropiado establecer soluciones singulares, técnicamente posibles, que prevén el acceso a contenidos encriptados caso por caso y sin establecer una regulación general que incida en los elementos internos de los sistemas de cifrado.

Se trataría, en definitiva, de aplicar técnicas de desencriptación sobre las comunicaciones concretas ya intervenidas o de buscar fórmulas alternativas que permitan acceder a su contenido en los momentos en que no está protegido por el sistema de cifrado.

La primera posibilidad que podemos incluir en lo que hemos denominado soluciones de intervención es la ejecutada mediante un ataque de suplantación.

Un ataque de suplantación, de intermediario o *man-in-the-middle attack,* consiste en conseguir que el emisor se comunique con el suplantador haciéndole creer que se está comunicando con el receptor, de modo que el intermediario, una vez accedido el contenido, lo retransmita al verdadero destinatario sin rastro alguno de la intervención suplantadora.

En el caso de comunicaciones cifradas con clave asimétrica[26], una vez suplantada la identidad del destinatario por el intermediario, el emisor cifra el contenido de la

[24] Esta es la solución prevista en los artículos 49 y siguientes de la *Regulation of Investigatory Powers Act* de Reino Unido. Sobre esta cuestión, véase B.B. CHATTERJEE, *New but not improved: a critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions*, en *International Journal of Law and Information Technology*, vol. 19, 3/2011, 264-284.

[25] Sobre la obligación de aportar las claves de cifrado y su relación con el derecho de no incriminación garantizado en la quinta enmienda a la Constitución estadounidense, *vid*. S. BRADY, *Keeping secrets*, cit., 325 y ss., y D. TERZIAN, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, en *UCLA Law Review Discourse*, 61/2014, 298-312.

[26] En los criptosistemas asimétricos la clave de codificación y la de descodificación son distintas, esto es, conociendo la clave de codificación se puede cifrar el mensaje, pero no sirve para descifrarlo. De este modo, cada comunicante posee dos claves criptográficas íntimamente relacionadas entre sí: una clave pública, conocida por todos, y una clave privada que solo conoce cada uno de ellos. El emisor utiliza la clave pública del destinatario para codificar el mensaje y éste lo desencripta con su clave privada. La relación entre las dos claves se asemeja a la que mantienen un candado y su llave. Conocer cómo cerrar el candado (clave pública) no te permite sin embargo abrirlo, sino que necesitarás tener la llave (clave privada). S. SINGH, *Los códigos secretos*, cit., 271.

comunicación utilizando la clave pública del intermediario, que éste puede descifrar utilizando su clave privada. A continuación, el intermediario transmite la información al destinatario verdadero cifrándola con su clave pública, para que éste la descifre con su clave privada y concluya el proceso comunicativo[27].

En resumen, el intermediario suplantador obtiene la información transmitida mientras que ambos interlocutores permanecen en la confianza de haber mantenido una comunicación reservada.

No obstante, esta forma de intervenir comunicaciones cifradas se tornará ineficaz si los interlocutores disponen de claves públicas certificadas por terceros, pues, cuando el emisor solicite al organismo certificador la clave pública del destinatario recibirá la clave del intermediario, lo que permitirá probar —indubitadamente— la suplantación[28].

La segunda posibilidad para acceder al contenido de comunicaciones encriptadas consiste en la intervención del mensaje cifrado y su conversión a texto descifrado aplicando técnicas de criptoanálisis.

El criptoanálisis es la ciencia matemática que se ocupa del análisis de los sistemas criptográficos con el objetivo de romper o eludir la protección que el sistema proporciona[29].

Aunque la ruptura de sistemas de cifrado con claves matemáticamente fuertes puede resultar en ocasiones ineficiente por su alto coste de tiempo o recursos, la incorporación de este tipo de funcionalidades a herramientas de interceptación de comunicaciones es cada vez más habitual.

Además, el actual desarrollo de la aplicación computacional de la física cuántica puede facilitar notablemente esta posibilidad. El principio de superposición de estados —los *qbits* o *bits cuánticos* pueden adoptar el estado 0, el estado 1 o los estados 0 y 1 a la vez— permite desarrollar varios procesos de forma simultánea en un ordenador, aumentando exponencialmente la capacidad computacional y haciendo inútil los sistemas criptográficos no cuánticos. La seguridad actual de los criptosistemas, fundada en la factorización matemática y considerada hoy indeleble a ataques de fuerza bruta (averiguación de la clave criptográfica mediante el método de prueba y error), podrá ser destruida en unos minutos[30].

Una última opción para sortear el cifrado consiste en practicar la intervención en aquellos momentos del proceso comunicativo en que las técnicas de encriptación no tienen incidencia en el contenido, lo que sucede bien accediendo a las albergadas en el dispositivo emisor, bien a las recibidas y descifradas en el del destinatario.

---

[27] J.L. MORENO FONTELA, *Servicios cifrados*, cit., 281.

[28] La combinación de esta medida con la imposición de deberes de colaboración puede permitir a la autoridad encargada de la investigación requerir a la autoridad de certificación la expedición de certificados falsos que avalen la suplantación; *vid*. J.L. MORENO FONTELA, *Servicios cifrados*, cit., 281.

[29] G. VIDAL y J.L. MORENO, *Cryptography and Communications Privacy: An Introduction*, en R. ALHAJJ and J. ROKNE (eds.), *Encyclopedia of Social Network Analysis and Mining*, New York, 2018, 513.

[30] G. MORALES LUNA, *Computabilidad y computación cuántica: revisión de modelos alternativos de computación*, en *Ingeniería Industrial*, 2/2011, 53; y A. RIVERA, *Computación cuántica: nuevas reglas del juego para los ordenadores*, en *Alfa. Revista de seguridad nuclear y protección radiológica*, 27/2015, 37.

Los sistemas comunicativos que incorporan cifrado extremo a extremo conservan por defecto los contenidos comunicados y ya descifrados en el dispositivo, salvo que se proceda a su borrado por parte de los interlocutores.

Por ello, es posible obtener los contenidos intercambiados accediendo a la fuente de origen o destino: ya sea antes de que la encriptación se produzca —en el sistema del emisor—, ya después de que la comunicación cifrada se convierta a texto claro —en el dispositivo receptor—.

Este acceso a los contenidos almacenados se puede llevar a cabo mediante el registro físico del dispositivo o mediante su registro remoto. En el primer caso, se practica sobre el contenido que contenga en el momento de su práctica el dispositivo o sistema estáticamente considerado. Por su parte, el registro remoto permite el examen dinámico de los contenidos alojados. A través de esta técnica se puede conocer no sólo el contenido del dispositivo en un momento determinado, sino también los archivos que se vayan añadiendo o suprimiendo durante el tiempo de observación[31].

La práctica de esta medida requiere el acceso al dispositivo mediante la introducción de un programa espía que permita a la autoridad encargada de su ejecución tomar el control del dispositivo objeto de examen. Normalmente este acceso se lleva a cabo aprovechando la conexión del dispositivo a una red pública o privada, valiéndose de canales abiertos de compartición de información —*bluetooth*, *NFC*, etc.— o mediante su incorporación oculta adjunta a una comunicación o archivo descargable; aunque, en ocasiones, será necesario manipular manualmente el dispositivo. La imposición de deberes de colaboración puede resultar de utilidad para facilitar asistencia técnica sobre posibles vías de acceso al terminal o para solicitar al prestador que abra una vía de penetración al troyano (por ejemplo, disponiendo restricciones a la protección del antivirus) [32].

6. *Conclusiones*

La generalización del uso de sistemas de cifrado implica una reacción a la actual situación de sobrevigilancia y su regulación constituye un reto de calado para los Estados.

La afección a diversos derechos fundamentales y los beneficios que se derivan de su utilización para determinados intereses de especial importancia deben ser tenidos en cuenta a la hora de hallar una solución dirigida a minimizar los riesgos que entraña. A la dificultad política y jurídica de tal empresa se adosa la complejidad técnica del objeto de regulación.

[31] Esta técnica ha sido la solución adoptada por el ordenamiento jurídico alemán para la intervención de comunicaciones cifradas. El art. 100.a) del Código Procesal Penal (*Strafprozessordnung*) permite «intervenir y grabar contenidos y datos de la comunicación almacenados en el sistema informático del investigado, si los mismos también hubieran podido ser intervenidos y grabados de forma encriptada mientras estuviera pendiente el proceso de transmisión en la red pública de telecomunicaciones».

[32] *Vid*. J.L. RODRÍGUEZ LAINZ, *Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción*, en *Diario La Ley*, 8896/2017, 2.

La principal conclusión es que no existe una fórmula mágica que permita a los Estados sortear los sistemas de cifrado. No obstante, las soluciones de intervención parecen resultar más eficaces y menos problemáticas que la regulación de los elementos internos de los elementos del cifrado o la imposición de deberes a fabricantes o usuarios.

Existen diversas posibilidades de intervenir con éxito comunicaciones encriptadas. La decisión de recurrir a una u otra de las técnicas aludidas dependerá de la eficacia y proporcionalidad de su uso en el caso concreto. Todas ellas pueden, además, completarse con la imposición jurídica de deberes de colaboración, como recurso de carácter transversal frente a eventuales dificultades en la intervención de comunicaciones cifradas.