InDret
1.2021

El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre

Hernán Blanco
Universidad Católica Argentina

Sumario

-

Mediante la Ley Orgánica 13/2015 se incorporaron en la Ley de Enjuiciamiento Criminal una serie de disposiciones referidas a medidas de investigación tecnológica (acceso remoto a sistemas informáticos, intervención de comunicaciones, vigilancia acústica y audiovisual, rastreo y localización) que habilitan el uso estatal de programas informáticos espías (spyware), en el marco de lo regulado en dichas disposiciones, para sostener las facultades legales de investigación frente a la nueva realidad tecnológica. Ello obliga a analizar, en especial, aspectos como el cumplimiento de los principios de proporcionalidad y especificidad en relación con el derecho a la intimidad, el contraste entre el derecho a confrontar la prueba de cargo frente a la confidencialidad de las herramientas informáticas empleadas y los problemas derivados de la posible implementación trasnacional.

Abstract

-

Pursuant to Organic Law 13/2015, a number of statutes regarding technological investigative measures were incorporated in Spain's Criminal Procedure Law (remote access to computer systems, communications interception, audio and video surveillance, location and tracking), which enable the use of spy computer programs (spyware) by the state in order to sustain its lawful investigative powers on account of the new technological reality. On account of that, it becomes necessary to assess aspects such as the compliance with the proportionality and particularity requirements in lieu of the right to privacy, the conflict between the accused's right to confront incriminating evidence and the confidentiality of the government's computer tools and the problems arising from any possible transnational application.

Title: *Court ordered hacking in Spanish procedural law after October 5th's Organic Law 13/2015*

-

Palabras clave: *Ley de Enjuiciamiento Criminal. Investigación penal. Spyware. Vigilancia estatal. Restricción de garantías fundamentales. Privacidad. Prueba electrónica*
Keywords: *Law of Criminal Procedure. Criminal investigation. Spyware. Governmental surveillance. Restriction of fundamental rights. Privacy. Electronic evidence.*

-

DOI: 10.31009/InDret.2021.i1.15

InDret

1.2021

Recepción
01/09/2020
-
Aceptación
31/10/2020
-

Índice

-

-

1. La necesaria incorporación de nuevas medidas de investigación y la reforma de la Ley de Enjuiciamiento Criminal*

En los últimos años, el mundo ha experimentado una verdadera revolución tecnológica que ha afectado tanto a las comunicaciones (telefonía móvil, correo electrónico, mensajería a través de internet) como a los medios técnicos que pueden ser utilizados para la investigación de hechos de apariencia delictiva[1]. Este salto tecnológico supone un revulsivo para todos los ámbitos de la sociedad, incluyendo naturalmente al jurídico. En efecto, resulta evidente que el Derecho no puede quedar al margen de la evolución de las nuevas tecnologías de la Información, puesto que estos últimos configuran un punto de referencia fundamental a tener en cuenta por el Estado de Derecho para saber compaginar los derechos e intereses de los ciudadanos con los avances tecnológicos[2].

En tal contexto, también el universo del Derecho penal, la actividad estatal de persecución de delitos y el Derecho procesal penal deben adaptarse al escenario planteado por la revolución en las Tecnologías de la Información y la Comunicación (en adelante, TICs), que han venido a modificar todos los aspectos de la vida de las sociedades modernas, incluyendo entre ellos el modo en que las personas delinquen y los sitios y modalidades en las que puede encontrarse la evidencia de esos delitos[3]. Es así que, en la actualidad, prácticamente todos los delitos que se pueden cometer en el mundo real encuentran su correlato en el mundo virtual, a los que vienen a añadirse los delitos propios del mundo virtual, como el sabotaje a sistemas informáticos, la entrada no autorizada en redes y sistemas, la difusión de material de terceros sin su consentimiento (tanto datos personales como íntimos), la distribución no autorizada de material protegido por derechos de autor o piratería informática, la distribución de ficheros de pornografía infantil, etc[4].

El trasvase de la actividad criminal del mundo físico al virtual acarrea, sin embargo, una nueva colección de desafíos para las autoridades encargadas de investigar y llevar a juicio a los responsables de dichas conductas, a la vez que engendra novedosos problemas de orden procesal vinculados a la necesidad de recalibrar el equilibrio entre los derechos fundamentales de los individuos con el interés del Estado en prevenir y perseguir los delitos. Así, por un lado, se advierte que -por ejemplo- la aparición de herramientas tecnológicas que habilitan la

* Autor de contacto: Hernán Blanco, hernanblanco72@gmail.com.

[1] Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", en CEDEÑO HERNÁN, M. (coord.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Navarra, págs. 21/47. Citado de documento informático obtenido en: https://zenodo.org/record/1042742#.Xx8aW55KjIU, pág. 2.

[2] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el Fortalecimiento de las Garantías Procesales y la Regulación de las Medidas de Investigación Tecnológica", en *Diario La Ley*, N° 8627, Sección Doctrina, 19/10/2015 (citado de documento electrónico obtenido en: https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMjcyMLY7Wy1KLizPw827DM9NS8klQAv991cyAAAAA=WKE).

[3] Cfr. LÓPEZ-BARAJAS PEREA, Inmaculada (2017): "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos", en *Revista de Internet, Derecho y Política*, N° 24, págs. 65/66.

[4] Cfr. RUBIO ALAMILLO, Javier (2015): "La informática en la reforma de la Ley de Enjuiciamiento Criminal", en *Diario La Ley*, Nº 8663 (citado de documento electrónico obtenido en: https://peritoinformaticocolegiado.es/blog/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/).

navegación anónima y limitan su trazabilidad han convertido en obsoletos los tradicionales sistemas de identificación de terminal e interceptación[5]; mientras que por el otro han surgido medios de investigación antes desconocidos, cuya utilización por el Estado puede suponer un peligro para el derecho de la persona o individuo al secreto de sus comunicaciones, a su libertad, y también a su intimidad[6].

Lo cierto es que la explosiva evolución de las TICs favorece que -incluso en regímenes democráticos y en el marco de sociedades que se presumen "libres" y respetuosas de los derechos individuales- las agencias estatales se encuentren en posición de explotar las herramientas tecnológicas que han ido surgiendo o desarrollándose para concretar una gigantesca expansión de su capacidad para monitorear las vidas de los ciudadanos, hasta alcanzar un nivel de detalle nunca antes visto[7]. Ello no implica, de por sí, que deba rechazarse '*ad limine*' el recurso a estos nuevos métodos de investigación, pero sí es necesario discutir cuál es el papel en el proceso del derecho a la autodeterminación en la información personal y qué fuerza cabe asignarles a las tradiciones procesales frente a las nuevas intromisiones en la información[8].

El legislador español ha efectuado un aporte fundamental en esta discusión mediante la reforma operada a través de la Ley Orgánica (en adelante, LO) 13/2015, de 5 de octubre[9], que ha venido, por un lado, a completar la regulación legal de la intervención de comunicaciones en la instrucción penal y, por otro, a regular por primera vez en la Ley de Enjuiciamiento Criminal[10] (en adelante, LEC) la utilización de medios tecnológicos avanzados en la investigación judicial de los hechos delictivos. Ello, mediante la introducción, en el Título VIII de la referida norma, de siete nuevos capítulos que regulan lo que la propia ley denomina "medidas de investigación tecnológica"[11]. En esa dirección, la nueva regulación pretende dotar de mayor eficacia al derecho procesal a la vez que se procura que se actúe con pleno respeto a las garantías del proceso, sobre todo, cuándo se pueden afectar los derechos fundamentales reconocidos en el art. 18 de la Constitución Española, aspecto que venía siendo ampliamente demandado tanto por la doctrina como por la jurisprudencia[12]. A la vez, se cumple, por medio de esta reforma de la LEC, España pasa a cumplir con las obligaciones que resultan de la ratificación del Convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001, que se aplica a la obtención de pruebas electrónicas y que ha dado cobertura legal a las medidas de investigación tecnológica[13].

---

[5] Fiscalía General del Estado (2013): Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, pág. 5.

[6] Cfr. RON ROMERO, José (2011): "Derecho al secreto de las comunicaciones telefónicas. Un reto para la buena administración" en *Anuario de la Facultad de Derecho de la Universidad de La Coruña*, N° 15/2011, pág. 105.

[7] Ver, al respecto, SWIRE, Peter / AHMAD, Kenesa (2011): "'Going dark' versus a 'golden age for surveillance'", CDT Fellows Focus Series, publicado el 28/11/2011.

[8] Cfr. HASSEMER, Winfried (2000), ¿Proceso penal sin protección de datos?, La insostenible situación del derecho penal, Ed. Comares, Granada, pág. 113.

[9] LO 13/2015, de 5 de octubre (BOE N° 239, de 6.10.2015).

[10] Real Decreto de 14 de septiembre de 1882 (BOE-A-1882-6036).

[11] Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", cit., pág. 2.

[12] Cfr. PÉREZ ESTRADA, Miren Josuné (2019): "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", en *Revista Brasileira de Direito Processual Penal*, Porto Alegre, Vol. 5, N° 3, pág. 1306.

[13] Cfr. PÉREZ ESTRADA, Miren Josuné (2019): "La protección de los datos personales…", cit., págs. 1306/1307.

En este escenario, el foco principal del presente trabajo habrá de centrarse en el que, a mi entender, resulta el aspecto más relevante de la LO 13/2015, que es el reconocimiento expreso, por parte del legislador español, de la facultad de las autoridades estatales de recurrir, como una medida más de investigación en el marco de un proceso criminal, al uso de programas espías (*spyware*). Ello, toda vez que, a partir de la experiencia recogida en los últimos diez o quince años en los EE.UU. y en el propio continente europeo, parece evidente que los referidos programas están llamados a convertirse en una de las herramientas más ubicuas y de mayor impacto en el arsenal de las agencias encargadas de la persecución de los delitos.

En tal contexto, se reseñan en primer lugar los antecedentes de uso de *spyware* en el Derecho comparado, la naturaleza de estas herramientas tecnológicas y los distintos métodos de empleo existentes, así como los usos que puede dársele a las mismas en el contexto de una investigación criminal. A continuación, se analizan las disposiciones contenidas en el nuevo título VIII de la LEC -que incluyen al registro de equipos informáticos, tanto en forma directa como a través de un ordenador en red o del acceso remoto mediante la instalación de *spyware*-; la interceptación de las comunicaciones (telefónicas, telemáticas o comunicaciones orales directas); el acceso a datos electrónicos ya almacenados (de contenido, de tráfico o asociados); la captación y grabación clandestina de imágenes tanto en espacios públicos como privados; la utilización de dispositivos de seguimiento y las operaciones mediante agente encubierto en la red-, a efectos de demostrar que todas ellas legitiman, en mayor o menor medida y con distintos alcances, la utilización de programas espías por parte del Estado. Por último, se pasa revista a las cuestiones problemáticas que se derivan de la introducción de esta clase de medidas de investigación tecnológica, en cuanto demanda un reajuste del equilibrio entre el interés estatal de contar con facultades que le permitan perseguir los delitos en aras de la seguridad de la sociedad, y los derechos fundamentales de los ciudadanos.

2. Antecedentes del hackeo legal en el Derecho comparado. Naturaleza y métodos

A partir de la reforma operada mediante la LO 13/2015, que es objeto de estudio en el presente trabajo, España ha pasado a ser -junto con Francia e Italia- uno de los pocos países de la Unión europea (y para el caso, del mundo) que regula expresamente el registro remoto de equipos informáticos a través de la instalación de un *software* espía como una medida de investigación criminal[14]. Sin embargo, y pese a la ausencia de regulación específica sobre la cuestión en la mayor parte del globo, lo cierto es que el uso de *malware* por parte de las agencias de investigación no es novedoso. Es así que el caso reportado más antiguo data de 2001, año en el cual el FBI instaló un *spyware* en el ordenador de un mafioso[15] a efectos de obtener las claves necesarias para acceder a un archivo encriptado almacenado dentro del mismo[16]. Ese mismo año se hizo público el desarrollo, por parte de dicha agencia, de un programa similar pero capaz

[14] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *Boletín del Ministerio de Justicia*, Madrid, Año LXXI, N° 2195, págs. 7/8.

[15] Cfr. MAYER, Jonathan (2016): "Constitutional malware", en *Social Sciences Research Network* (SSRN), publicado el 14/11/2016, pág. 5.

[16] Ver: *United States v. Scarfo*, 180 F. Supp. 2d 572 (Corte del Distrito de New Jersey, 2001). Lo que se instaló es un programa "keylogger" (identificado en el caso como "Keylogger System" o KLS), que registra todo lo que el sujeto teclea.

de ser instalado de manera remota en el equipo informático del sujeto investigado, al que se bautizó como "Linterna mágica" ("*Magic Lantern*"). Luego, en junio de 2007 se conoció la existencia de un nuevo programa espía también instalable en forma remota, el CIPAV (siglas de "*Computer and Internet Protocol Adress Verifier*" o "Verificador de direcciones de Computadora y Protocolo de Internet"), que envía a través de la Red a otro ordenador (controlado por la autoridad que lleva a cabo la investigación) la información recogida del dispositivo investigado[17].

Contemporáneamente a la aparición del CIPAV en los EE.UU., en 2007 el Ministerio del Interior Alemán anunció que se había diseñado su propio spyware estatal[18] al que denominó "*Software* de Interceptación Remota de Comunicaciones" (RCIS, también llamado "*Staatstrojaner*" o "*Bundestrojaner*"). En principio, el uso de esta herramienta se autorizó únicamente para la interceptación de comunicaciones en tiempo real a través de Skype u otras vías similares, programas de mensajería instantánea o correos electrónicos[19]. Ese mismo año, el Tribunal Supremo Alemán (BVerfG) declaró inconstitucional una norma sancionada en ese país en 2007, que autorizaba el uso de *spyware* para monitorear el contenido de computadoras[20]. También en Italia se registró el uso, en el marco de investigaciones criminales, de programas espías a los que se aludió con varias denominaciones incluyendo "*captatore informatico*", "*agente intrusore*" o directamente "*troiano*"[21]. Finalmente, existen indicios sobre el uso de programas troyanos como herramientas en investigaciones criminales (o en casos de espionaje estatal) tanto en Gran Bretaña como en Portugal.

En lo tocante a la regulación de la utilización de este medio de investigación tecnológica, las principales iniciativas supranacionales comenzaron a desarrollarse a partir de la sanción de la Convención de Budapest. Así, en el mes de diciembre de 2008, la Comisión Europea y la Unión Internacional de Telecomunicaciones iniciaron el proceso de armonización sobre legislación de políticas de CTI y procedimientos regulatorios en el Caribe (HIPCAR, por sus siglas en inglés), a fin de procurar la uniformización de la legislación en los países de la Comunidad del Caribe (CARICOM). El resultado fue, posiblemente, el modelo legislativo más detallado a nivel mundial en materia de cibercrimen y evidencia digital[22]. En especial, cabe hacer mención al artículo 27 del Modelo de Lineamientos de Regulación y Textos Legislativos sobre Cibercrímenes[23] que incorpora en su inc. 1° la autorización para "*…el uso de software forense remoto con la finalidad específica requerida por la investigación e instalarlo en el sistema informático del sospechoso para recolectar la evidencia relevante*".

---

[17] Cfr. ORTIZ PRADILLO, Juan Carlos (2009): "El 'remote forensic software'…", cit., pág. 3.

[18] Cfr. Der Spiegel: "Electronic surveillance scandal hits Germany", publicado el 10/10/2011, obtenido en: http://www.spiegel.de/international/germany/the-world-from-berlin-electronic-surveillance-scandal-hits-germany-a-790944.html.

[19] Cfr. DAHLMANN, Anja (2016): "E-evidence and cross border data requests in Germany", en DE ZAN, Tommaso / AUTOLITANO, Simona (editores), *EUnited against crime: Improving criminal justice in European Union cyberspace,* Instituti Affari Internazionali, págs. 30/31.

[20] A pesar de lo resuelto por el BverFG, en 2011 surgieron reportes sobre el uso del "Bundestrojaner" ("troyano federal") en al menos 50 ocasiones, y no sólo en los supuestos -muy limitados- autorizados en el fallo aludido (Al respecto, ver: SILVA RAMALHO, David: "The use of malware…", cit., pág. 63).

[21] Cfr. DE ZAN, Tomasso (2016): "E-evidence and cross border data requests in Italy", en DE ZAN, Tommaso / AUTOLITANO, Simona (editores), *EUnited against crime: Improving criminal justice in European Union cyberspace,* Instituti Affari Internazionali, pág. 47.

[22] Cfr. SILVA RAMALHO, David (2014): "The use of malware as a means of obtaining evidence in Portuguese criminal proceedings", en *Digital Evidence and Electronic Signature Law Review*, Vol. 11, págs. 65/66.

[23] Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts.

El elemento en común entre un eventual spyware estatal y la generalidad de los programas maliciosos (*malware*) es que ambos apuntan a explotar las denominadas "vulnerabilidades" de los sistemas informáticos. El término alude a debilidades o errores existentes en dichos sistemas, susceptibles de ser aprovechadas por un tercero no autorizado para dejar expuesto algún aspecto de dicho sistema[24]. La aparición de estas vulnerabilidades se vincula con un principio básico de la ingeniería de *software* que es que los defectos ("*bugs*") *suceden*[25]. En la práctica, cualquier imperfección en el código puede resultar en la aparición de un defecto. Este defecto rara vez se manifestará, pero eso no implica que no exista. Y si se da en una sección crítica -en términos de seguridad- del código, el resultado puede ser una vulnerabilidad[26]. A mayor complejidad de los sistemas informáticos, más alta es la tendencia a la aparición de vulnerabilidades. Ello así, desde que el referido incremento determina que su funcionamiento acabe excediendo lo que sus creadores pudieron predecir o simular, y exhibir resultados sorprendentes o impredecibles. Esto es lo que explotan los hackers: la posibilidad de hacer que los programas funcionen de un modo para el cual no han sido pensados o diseñados[27].

Las vulnerabilidades de los sistemas informáticos se explotan mediante el desarrollo de los denominados "*exploits*", que son básicamente las herramientas con las que se obtiene el acceso no autorizado a un sistema vulnerable. Los *exploits* pueden ser programas, o simplemente un conjunto de comandos o acciones[28]. Las oportunidades para desarrollar *exploits* son múltiples, toda vez que se descubren nuevas vulnerabilidades explotables en programas de uso generalizado casi a diario[29]. De estas, las más valiosas son las denominadas "vulnerabilidades de día cero". Esto es: aquellas que son descubiertas y pueden ser explotadas antes de que el desarrollador del *software* que la contiene (y el público en general) sepa de su existencia[30] para poder resguardarse.

En tal contexto, el uso estatal de *spyware* como método de investigación supone, en esencia, que las autoridades recurran a las mismas técnicas empleadas por los *hackers* o "*crackers*" (entendidos como quienes acceden sin autorización a un equipo o sistema informático), sólo que con una finalidad distinta: obtener evidencia que pueda ser relevante para acreditar la

[24] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2014): "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet", en *Northwestern Journal of Technology and Intellectual Property*, Vol. 12, N° 1, págs. 22/23).

[25] Existen oportunidades de sobra para que éstos aprovechen. En promedio, existen entre 15 y 50 defectos cada 1000 líneas de código en el software. Las aplicaciones más utilizadas en la actualidad contienen *millones de líneas de código*. Y a medida que su complejidad se incrementa, también los defectos potenciales (ver: PELROTH, Nicole (2016): "Software as weaponry in a computer-connected world", en *The New York Times*, publicado el 7/6/2016, obtenido en: http://www.nytimes.com/2016/06/09/technology/software-as-weaponry-in-a-computer-connected-world.html?).

[26] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2014): "Lawful hacking…", cit., pág. 27.

[27] Cfr. CLARKE, Zuley / CLAWSON, James / CORDELL, María (2013): "A brief history of hacking", en *Historical approaches to digital media*, Georgia Tech University, LMC 6316, pág. 2.

[28] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2014): "Lawful hacking…", cit., pág. 23.

[29] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2013): "Going bright…", cit., pág. 67.

[30] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2014): "Lawful hacking…", cit., pág. 23. Según explican los autores, en muchos casos los desarrolladores recién se enteran de la existencia de este tipo de vulnerabilidades cuando el sistema ya ha sido comprometido.

comisión de un delito y la culpabilidad de quienes lo cometieron. En ese aspecto, la técnica objeto de análisis no difiere de la interceptación subrepticia de una comunicación telefónica, que también es ilícita cuando se lleva a cabo con un propósito ilegítimo y sin habilitación judicial. Esto es: se trata, en ambos supuestos, de una intrusión en espacios de reserva de la intimidad de los ciudadanos, que sólo puede ser considerada aceptable cuando encuentra justificación en la necesidad de recurrir a ella para prevenir o perseguir un delito, en defensa de la comunidad en general.

La divergencia en los fines no sólo determina la legitimidad de la medida, sino también el modo en que debe funcionar el programa espía estatal, toda vez que, a diferencia de los hackers, que pueden dirigir su accionar contra blancos "de oportunidad" (es decir, cualquiera que aparezca vulnerable), el Estado sólo puede utilizar el *spyware* con relación a los individuos mencionados en la autorización judicial respectiva. Ello demanda el uso de herramientas de interceptación especializadas, cuyo funcionamiento debe superar el estándar meramente "probabilístico" de los programas clandestinos. En efecto, el *malware* estatal debe tener una alta probabilidad de comprometer exitosamente el equipo de su objetivo sin alertarlo y sin perturbar el funcionamiento de ese equipo ni de ningún otro. Además, debe permitir que quienes lo operan confirmen rápidamente si ha tenido éxito o no, que se lo controle durante el tiempo que dure la intervención legalmente autorizada y que pueda ser eliminado sin dejar rastros una vez que aquella concluya[31].

En dicho escenario, el desarrollo de un *spyware* estatal debe contemplar cuatro elementos primarios: a) la selección o descubrimiento de la vulnerabilidad subyacente; b) el mecanismo de instalación; c) el mecanismo de acceso al contenido buscado; y d) el modo de envío de los datos capturados a los investigadores[32]. De igual manera, una eventual operación de hackeo estatal normalmente habrá de dividirse en cuatro pasos: 1) el envío ("*delivery*") del spyware al objetivo, 2) la intrusión ("*exploitation*") en el sistema informático, 3) la ejecución ("*execution*") del programa espía y 4) el "reporte" ("*reporting*")[33], es decir el envío de los datos obtenidos por el spyware, ya sea a la agencia gubernamental encargada del monitoreo o a la propia autoridad judicial que ordenó la intervención[34].

Para concretar una medida de investigación mediante el uso de un *spyware* estatal puede recurrirse a dos métodos principales. Por un lado, el ataque de "ingeniería social" ("*social-engineering*"[35]); por el otro, el ataque de "abrevadero" ("*watering hole*"). El primero consiste en la utilización de algún ardid o engaño (por ejemplo, enviar un correo electrónico que provenir de una fuente confiable o ser inocuo) para conseguir que el objetivo *acepte ejecutar una acción*

[31] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2013): "Going bright: Wiretapping without weakening communications infrastructure", en *IEEE Security & Privacy*, Vol 11, N° 1, pág. 66.

[32] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2013): "Going bright…", cit., pág. 66.

[33] Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., pág. 13.

[34] En mayor detalle, sobre los aspectos técnicos del desarrollo de una herramienta de hackeo estatal, ver: BLANCO, Hernán (2020), *Tecnología informática e investigación criminal*, La Ley, Buenos Aires, págs. 102/118.

[35] Este concepto engloba a todas las modalidades basadas en el engaño y la persuasión, utilizados para obtener información significativa o lograr que la víctima realice un determinado acto. En más detalle, sobre el tema, ver: MITNICK, Kevin D. / SIMON, William L. (2002), *The art of deception. Controlling the human element of security*, John Wiley & Sons, New Jersey.

que se le sugiere, como abrir un archivo adjunto o clickear en un link contenido en el mensaje[36]. El segundo método consiste en alterar el funcionamiento de una página web que el/los objetivo/s puede/n llegar a visitar para que "fuerce" a los ordenadores que se conecten con ella a enviar la información relevante a los servidores de los investigadores[37]. De este modo, la página web contaminada con el *spyware* estatal hace las veces del "abrevadero" al que se acercan las "presas", permitiendo que sean atacadas mediante el programa espía. De esto último se sigue, en consecuencia, que los ataques "de abrevadero" –a diferencia de los de "ingeniería social"- por lo general se desarrollan en el marco de una operación encubierta estatal en la que una vez detectada la ubicación de una página web ilegal -por ejemplo una dedicada a la difusión de imágenes de explotación sexual infantil-, las autoridades en lugar de sacarla de línea toman control de la misma y permiten que siga funcionando, solo que incluyendo dentro de su sistema operativo el *malware* estatal, el cual se programa para introducirse en los ordenadores de todos los visitantes que ejecuten una determinada acción (como por ejemplo descargar imágenes ilícitas). No se trata, pues, de enviar el *spyware* a individuos específicos, sino infectar los equipos de todos aquellos que visiten la página y ejecuten la acción que dispara la descarga del programa estatal[38].

3. Usos posibles del hackeo legal

La ubicuidad de la informática en las acciones de la vida diaria en las sociedades modernas, el carácter de herramienta imprescindible que han adquirido los ordenadores y -en especial- los modernos teléfonos móviles y la flexibilidad de los programas espías determina que éstos últimos puedan ser utilizados para llevar a cabo una amplia gama de medidas de investigación y monitoreo en el marco de procesos criminales. Así, las autoridades estatales pueden recurrir al *spyware* para acceder remotamente a datos almacenados, para obtener claves de acceso a documentos encriptados o que se encuentran en servidores externos, para monitorear comunicaciones realizadas a través de la Internet, para realizar vigilancias acústicas o audiovisuales, para localizar e individualizar a las personas que se contactan con determinadas páginas o individuos a través de la red y para rastrear en tiempo real a sujetos sometidos a investigación.

Con respecto al primero de los usos aludidos (acceso remoto a datos almacenados), cabe señalar que una de las principales consecuencias del hecho de que en la actualidad, las tecnologías de la información y las comunicaciones tengan algún grado de injerencia (directa o indirecta) en la casi totalidad de las actividades humanas es que cada vez más información relacionada con dichas actividades (incluyendo, por supuesto, a las que infringen la ley penal) se almacena digitalmente en alguno de los múltiples formatos existentes (discos rígidos, discos extraíbles, servidores externos, pendrives, CDRs o DVRs y un largo etcétera). Habida cuenta de que esta evidencia digital puede resultar tanto o más importante que la evidencia física para esclarecer hechos delictivos, identificar a los responsables y otorgar sustento a una eventual condena, es imprescindible contar con medios efectivos para poder obtenerla de un modo que permita su presentación y valoración en el proceso penal.

[36] Cfr. LERNER, Zach (2017): "A warrant to hack: An analysis of the proposed amendments to rule 41 of the Federale Rules of Criminal Procedure", en *Yale Journal of Law and Technology*, Vol. 18, N° 1, págs. 40/41 (énfasis añadido).
[37] Cfr. LERNER, Zach (2017): "A warrant to hack…", cit., pág. 41.
[38] Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., págs. 13/14 (énfasis añadido).

En orden a ello, la primera cuestión a sopesar es que, como bien explican KOOPS y GOODWIN, los datos informáticos y los objetos físicos son "animales diferentes", siendo que los primeros son múltiples además de móviles y a la vez accesibles remotamente en forma instantánea. Ello apareja varias consecuencias que distinguen a las "ciber investigaciones" de las pesquisas tradicionales. Los datos son esencialmente volátiles y pueden ser desplazados a miles de kilómetros con unos pocos clicks en el mouse; también son vulnerables, pudiendo ser modificados o removidos con facilidad. Por consiguiente, el riesgo de que este tipo de evidencia sea eliminada o alterada es mucho mayor, lo que determina que resulte esencial *recolectar toda la prueba posible ni bien comienza la investigación*, incluso extendiendo el alcance de una medida cuando se toma conocimiento de que la información no está almacenada localmente (en la computadora personal del sospechoso, por ejemplo) sino en un servidor externo[39].

Ahora bien: como contrapartida, vale tener presente que uno de los principales cambios que trajo consigo la evolución tecnológica reside en la posibilidad de desconectar la ubicación del agente gubernamental que lleva a cabo el registro y secuestro de evidencia del lugar físico en que se encuentran los datos objeto de la medida[40]. Ello, toda vez que las herramientas tecnológicas actualmente disponibles permiten al Estado obtener "a distancia" datos de archivos almacenados en la memoria de los equipos sometidos a una medida de investigación sin necesidad de tener ningún tipo de contacto físico con ellos. Por consiguiente, estos nuevos programas implican un cambio sustancial en la forma de obtener datos que se encuentran alojados en un soporte informático.

Uno de los modos en los que puede accederse a la evidencia informática sin tomar contacto *físico* con el soporte que la almacena es recurrir a un programa informático específicamente diseñado[41] que se introduce en el ordenador (o el smartphone) del sospechoso sin su conocimiento. Este programa luego procede a copiar la información almacenada en el equipo y la transfiere a la autoridad a cargo de la investigación para su análisis. Es, por ende, muy similar a los programas "troyanos" utilizados por los *hackers*, que también se usan para extraer información personal[42]. La ventaja que ofrece el recurso a esta herramienta tecnológica es que puede ser instalada en forma clandestina y sin necesidad de acceder al domicilio o al entorno físico del sospechoso, que de ese modo no es alertado sobre la existencia de una investigación en su contra, como si ocurre cuando se produce un registro físico de su morada[43].

Asimismo, el uso de un spyware estatal facilita la obtención de la información digital que el imputado pueda haber almacenado en la "nube" (esto es: en servidores externos cuyo espacio de almacenamiento le es ofrecido a los usuarios como servicio), ya que mediante a esta clase de programas es posible acceder a cualquier equipo que esté conectado a la Internet. En esa

[39] Cfr. KOOPS, Bert-Jaap / GOODWIN, Morag (2014): "Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law", *Tilburg Law School Legal Studies Research Paper* Series N° 5/2016, pág. 18 (énfasis añadido).

[40] Cfr. DASKAL, Jennifer (2015); "The un-territoriality of data", en *The Yale Law Journal*, Vol. 125, N° 2, págs. 369/370.

[41] Según la jurisdicción, se alude a estas herramientas informáticas como "remote forensic software" (software forense remoto o RFS) o una "network investigative technique" (técnica de investigación en red o NIT), entre otras denominaciones.

[42] De allí que, en Alemania, se aludiese coloquialmente al spyware estatal como "troyano federal".

[43] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court on the right in confidentiality and integrity of information technology systems – a case report on BVerfG, NJW 2008, 822", en *Scripted*, Vol. 6, N° 1, pág. 109.

dirección, el incremento en el uso de los servicios de almacenamiento en la nube por parte de empresas y particulares supone otra ventaja para los investigadores estatales, desde que le ofrece la posibilidad de hacerse de datos que de otro modo nunca se hubiesen generado o habrían sido guardados en elementos fáciles de ocultar como tarjetas de memoria o flash drives (los cuales, por consiguiente, hubiesen tenido que ser hallados y accedidos físicamente para poder recolectar dicha información subrepticiamente)[44].

Por añadidura, el empleo de programas espías permite sortear uno de los principales problemas que surgen a la hora de obtener evidencia digital "en reposo", que reside en el uso cada vez más habitual de herramientas de encriptación "fuerte"[45] para impedir el acceso de terceros a los datos almacenados. Al respecto, vale aclarar que de este modo no se obsta a que el tercero pueda apropiarse de los datos (esto es: copiarlos o traspasarlos de la unidad de almacenamiento del propietario a una propia), pero si a que pueda conocer lo que contienen, ya que se encuentran cifrados.

En los últimos años, la proliferación de herramientas de encriptación seguras baratas o incluso gratuitas (como TrueKrypt, BitLocker o Pretty Good Privacy) le ofrece tanto a los ciudadanos comunes como a los delincuentes una capacidad sin precedentes para mantener en secreto su información privada. Hoy, incluso una persona con mínimos conocimientos sobre el manejo de computadoras tiene el poder de resguardar sus datos confidenciales tras una barrera infranqueable de protección[46]. De hecho, en muchos equipos la encriptación está habilitada *por defecto*, lo cual -como explica HENNESEY- reduce considerablemente el nivel técnico requerido para participar en actividades ilícitas a través de Internet[47]. A consecuencia de ello, el uso de estas herramientas por parte de terroristas, narcotraficantes, distribuidores y consumidores de explotación sexual infantil, ciberdelincuentes, criminales de cuello blanco y toda clase de delincuentes ha crecido exponencialmente, impidiendo o dificultando el acceso de las autoridades estatales a la información que podría conducir a probar sus delitos[48].

---

[44] Cfr. SPOENLE, Jan (2010): "Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal", *Council of Europe Discussion Paper* N° 31, pág. 6.

[45] A nivel técnico se distingue entre encriptación convencional y "encriptación fuerte", siendo esta última la que se basa en algoritmos probados y aceptados por la industria, que contienen claves extensas (un mínimo de 112 bits) y procedimientos de manejo de claves apropiados (conforme definición del PCI Security Standards Council, organización dedicada a la seguridad de la información de las tarjetas de crédito, una de las principales usuarias de protocolos de encriptación fuertes, ver: https://searchsecurity.techtarget.com/definition/strong-cryptography).

[46] Cfr. ATWOOD, J. Riley (2015): "The encryption problem: Why the courts and technology are creating a mess for law enforcement", en *Saint Louis University Law Review*, Vol. 34, pág. 407.

[47] Cfr. HENNESSEY, Susan (2017): "The elephant in the room: Addressing child exploitation and going dark", *Aegis Paper Series*, Hoover Institution, Stanford University, N° 1701, pág. 7 (énfasis en el original).

[48] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., pág. 7. A modo de ejemplo, la oficina del Fiscal del Distrito de Nueva York informó que entre septiembre de 2014 y marzo de 2016 registraba 175 casos en los que los investigadores se vieron impedidos de obtener evidencia por no poder acceder a la información digital contenida en equipos secuestrados (Cfr. KAMINSKI, Liz (2018): "Calling a truce to the Crypto Wars: Why Congress and tech companies must work together to introduce new solutions and legislation to regulate encryption" en *Seton Hall Law Review,* Vol. 48, N° 2, págs. 518/519). Al respecto, en una compulsa realizada por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en 2013, entre el 60 y el 80% de los países de todas las regiones (salvo Asia y Oceanía) reportaron el uso de encriptación en la evidencia digital obtenida en sus investigaciones. Muchos de esos señalaron también que se verificaba un *aumento* en el empleo de dicha herramienta informática (ver: UNODC (2013), *Comprehensive study on cybercrime*, United Nations, Nueva York, págs. 163/164).

En tal contexto, el uso herramientas informáticas permite recolectar los datos que de otro modo estarían encriptados en formato "*plaintext*", al captarlos cuando el usuario los está tipeando o trabajando con el archivo. En su defecto, se puede obtener la contraseña (clave criptográfica) para poder desencriptarlos con posterioridad[49]. Esto último puede lograrse recurriendo a una modalidad de spyware conocida como "*keylogger*" (registrador de teclas), que como su nombre lo indica registra (e informa) todo lo que ha tecleado el usuario en el ordenador, incluyendo las contraseñas con las que se desencripta la información. En esta dirección, VELASCO NUÑEZ destaca que esta "técnica novedosa" puede resultar útil ante la necesidad de captar actuaciones interactivas no monitorizables en el investigado (especialmente su clave y contraseña), en la medida en que se disponga su instalación con autorización judicial, como complemento técnico de lo que jurídicamente es la interceptación de la información de interés para la investigación en los ordenadores[50].

Por otra parte, el recurso al *spyware* le sirve el Estado para garantizar la plena vigencia no ya de su facultad legal para intervenir las comunicaciones de los ciudadanos (que no se encuentra en duda) sino de capacidad *fáctica* de lograrlo. Esto es, la denominada "interceptabilidad técnica", entendida como la posibilidad de que aquellas puedan ser técnicamente interceptadas en la red de telecomunicaciones o el servicio que transporta la comunicación[51]. Esta última se ve amenazada por los cambios operados en las comunicaciones realizadas por medio de teléfonos móviles, motorizados por la generalización del uso de los denominados teléfonos "inteligentes" (*smartphones*) con acceso a la Internet y la aparición de servicios (muchos de ellos gratuitos) que reemplazan a la telefonía móvil tradicional por formas de comunicación alternativas, a través de la Red[52].

Las nuevas modalidades de comunicación a través de Internet ponen en jaque la imperceptibilidad técnica de las comunicaciones por dos motivos distintos. Por un lado, la adopción de una arquitectura técnica que abandona el modelo de comunicación "intermediada", que constituye la base del sistema actualmente vigente de intervención de las comunicaciones telefónicas. Por el otro, la encriptación de los datos transmitidos a través de Internet.

Al respecto, cabe tener presente que el sistema "tradicional" de telefonía (tanto de línea como celular) está conformado a partir de un sistema de "Red Telefónica Pública Conmutada" (en adelante, RTPC)[53], en el cual *todas las llamadas telefónicas son establecidas a través de un conmutador central* que es el que dirige la llamada saliente hacia su destino buscado (el teléfono del receptor de la llamada, identificado por su número de línea). En tal contexto, la modalidad utilizada para concretar la interceptación estatal consiste, en esencia, en establecer un sistema

[49] Esto es: la solución al algoritmo criptográfico utilizado para encriptar los contenidos, que funciona como contraseña para revertir el proceso y acceder a la información en formato "*plaintext*".
[50] Ver: VELASCO NUÑEZ, Eloy (2011): "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías" en *Revista de Jurisprudencia*, N° 4, citado de documento electrónico obtenido en: https://elderecho.com/novedades-tecnicas-de-investigacion-penal-vinculadas-a-las-nuevas-tecnologias.
[51] Cfr. KOOPS, Bert-Jaap / BEKKERS, Rudi (2017): "Interceptability of telecommunications: Is US and Dutch law prepared for the future?", en *Telecommunications Policy*, Vol. 31, pág. 46.
[52] Cfr. GOLDE, Nico / REDON, Kevin / BORGAONKAR, Ravishankar (2012): "Weaponizing femtocells: The effect of rogue devices on mobile telecommunication", en *Network and Distributed System Security Symposium* (NDSS), publicado el 6/2/2012, documento informático obtenido en: https://www.tu-berlin.de/fileadmin/fg214/Papers/femto_ndss12.pdf, pág. 1.
[53] Traducción de lo que se conoce, en idioma inglés, como *Public Telephone Switched Network* (PTSN).

mediante el cual las capacidades para generar "llamadas en conferencia" de los conmutadores centrales se adaptan para convertir a las comunicaciones intervenidas en llamadas en conferencia, en las que participa un oyente silencioso subrepticio (el Estado)[54].

En este escenario, la mayoría de las normas existentes a nivel internacional con relación a la interceptación de comunicaciones telefónicas (incluyendo las de España) siguen el modelo establecido por los EE.UU. en la "*Communications Assistance for Law Enforcement Act*" (Ley de Asistencia a la Persecución de Delitos en materia de Comunicaciones, o CALEA por sus siglas en inglés), que estableció la obligación de las empresas de telecomunicaciones de implementar interfaces que permitiesen la interceptación legal de las comunicaciones en todos los conmutadores locales[55]. En esencia, lo que CALEA les impuso a dichas compañías es la obligación de diseñar e implementar soluciones en las redes a su cargo para garantizar la capacidad del Estado de interceptar comunicaciones en los casos en los que la ley lo autoriza. Esto es: la ya mencionada interceptabilidad técnica.

Siguiendo la línea trazada por CALEA, el Consejo de Ministros de Justicia e Interior de la Unión Europea adoptó en enero de 1995 una resolución sobre la "Interceptación Legal de Telecomunicaciones" que requirió a los estados miembros la adopción de legislación que impusiera requisitos de interceptabilidad a los proveedores de servicios de telecomunicaciones[56]. En España, primero en la ley 32/2003 de 3 de noviembre[57] (hoy derogada) y luego en la actual ley 9/2014, de 9 de mayo[58], se estableció que los operadores del sistema "*…están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes*"[59]. En dicho marco, se puso en funcionamiento para dar curso a las interceptaciones telefónicas el "Sistema Informático Integrado de Interceptación Legal de Telecomunicaciones" (en adelante, SITEL), utilizado conjuntamente por las Direcciones Generales de Policía y Guardia Civil[60]. Al respecto, vale aclarar que SITEL no lleva a cabo por sí mismo las interceptaciones, sino que fue concebido para canalizar de modo seguro las concretadas por los propios operadores. Es decir que, como explica RON ROMERO, quien baja el interruptor para poder escuchar es la operadora, no la policía judicial ni el Juez autorizante[61].

La primera variación tecnológica cuya aparición puso en crisis el enfoque tradicional para la interceptación del contenido de las comunicaciones fue el surgimiento de los sistemas de "*Voice over Internet Protocol*" ("Voz sobre Protocolo de Internet" o VoIP)[62]. Existe gran variedad

[54] Cfr. BELLOVIN, Steven / BLAZE, Matt / BRICKELL, Ernest / BROOKS, Clinton / CERF, Victor / DIFFIE, Whitfield / LANDAU, Susan / PETERSON, Jon / TREICHLER, John (2006): "Security implications…", cit., pág. 5.
[55] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2014): "Lawful hacking…", cit., pág. 1.
[56] Cfr. KOOPS, Bert-Jaap / BEKKERS, Rudi (2014): "Interceptability of telecommunications…", cit., pág. 49.
[57] Ley 32/2003, de 3 de noviembre (BOE N° 264, de 4.11.2003).
[58] Ley 9/2014, de 9 de mayo (BOE N° 114, de 10.5.2014).
[59] Art. 36.2 de la Ley 9/2014.
[60] Cfr. RON ROMERO, José (2011): "Derecho al secreto de las comunicaciones telefónicas…", cit., pág. 118.
[61] Cfr. RON ROMERO, José (2011): "Derecho al secreto de las comunicaciones telefónicas…", cit., pág. 121.
[62] Cfr. BELLOVIN, Steven / BLAZE, Matt / BRICKELL, Ernest / BROOKS, Clinton / CERF, Victor / DIFFIE, Whitfield / LANDAU, Susan / PETERSON, Jon / TREICHLER, John (2006): "Security implications…", cit., págs. 2/3 (énfasis

de aplicaciones VoIP disponibles para los diferentes equipos móviles y sistemas operativos (Android, iOS, Windows Mobile, Symbian y Blackberry)[63]. La mayoría de los servicios -empezando por el más famoso, Skype- son gratuitos[64] y, en general, muy simples de instalar y usar. Sólo hace falta descargar el software, elegir una identificación y a partir de allí, donde quiera que exista una conexión de Internet se puede efectuar una llamada "telefónica"[65].

El problema de los sistemas VoIP, en orden a la interceptabilidad técnica, reside en la ausencia de un punto fijo en el cual establecer la interceptación (esto es: la característica central que facilita las intervenciones en la RTPC). Dicha ausencia refleja uno de los elementos esenciales de la Internet, que es que cualquier nodo con suficiente ancho de banda puede funcionar como proveedor del servicio. De allí que servicios como Skype carezcan de servidores centrales: se trata de una red distribuida, basada en el sistema "par a par" ("*peer-to-peer*" o P2P)[66]. El concepto de P2P se sustenta en la idea de que el usuario que necesita algún dato puede conectarse directamente con el usuario que *tiene* ese dato, y que la función de la red tan solo es permitir que ello ocurra, ofreciendo servicios de directorio -la versión P2P del Servicio de Nombres de Dominios (DNS, por sus siglas en inglés) que convierte los números de IP en nombres de dominio[67]- provistos por actores ("*hosts*") elegidos o designados dentro de la red[68].

Es importante destacar que la carencia señalada no puede resolverse mediante la sanción de una ley, similar a CALEA, que procure extender las capacidades de interceptación legal a estos sistemas, toda vez que ello requeriría o bien convertir a los servicios VoIP en una copia del RTPC, o introducir serios riesgos de seguridad en las aplicaciones VoIP locales[69]. A lo que cabe añadir que, dada la disponibilidad de servicios de esa clase accesibles mediante Internet desde cualquier lugar del mundo, cualquier regulación en tal sentido se encontraría con prestadores basados en el extranjero que no estarán sometidos a la misma, pero que de todos modos podrán

---

añadido). Al respecto, los autores explican que, en realidad, el término VoIP no alude a *un* servicio sino a una amplia gama de posibles servicios. Fundamentalmente, se trata de una aplicación para transmitir en tiempo real a través de la Internet, información de audio como la voz humana, emulando el servicio telefónico tradicional. A tal efecto, se apoya en un principio fundamental de la Red, según el cual cualquier ordenador con una dirección de IP puede enviar cualquier tipo de datos que se le indique enviar a cualquier otro ordenador con una dirección de IP. Lo único que se requiere es una conexión de Internet y un programa en ambos ordenadores capaz de codificar y transmitir los datos.

[63] Cfr. AZFAR, Abdullah / CHOO, Kim-Kwang Raymond / LIU, Lin (2014): "A study of ten popular Android mobile VoIP applications: Are the communications encrypted?", en *47th Annual Hawaii International Conference on System Sciences* (HICSS 2014), IEEE Computer Society Press, pág. 3.

[64] Cfr. KOOPS, Bert-Jaap / BEKKERS, Rudi (2014): "Interceptability of telecommunications…", cit., pág. 59.

[65] Cfr. BELLOVIN, Steven / BLAZE, Matt / BRICKELL, Ernest / BROOKS, Clinton / CERF, Victor / DIFFIE, Whitfield / LANDAU, Susan / PETERSON, Jon / TREICHLER, John (2006): "Security implications…", cit., pág. 2.

[66] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2013): "Going bright…", cit., pág. 65.

[67] Las que funcionan, en la práctica, como los antiguos directorios telefónicos, solo que con direcciones de IP en lugar de números telefónicos.

[68] Cfr. JOHNSON, M. Eric / MCGUIRE, Dan / WILLEY, Nicholas D. (2008): "The evolution of the peer-to-peer file sharing industry and the security risk for users", en *41 st. Hawaii International Conference on System Sciences, Institute of Electrical and Electronic Engineers (IEEE)*, documento informático obtenido en: https://pdfs.semanticscholar.org/3fa2/84afe4d429c0805d95a4bd9564a7be0c8de3.pdf, pág. 2 (énfasis añadido).

[69] Cfr. BELLOVIN, Steven / BLAZE, Matt / BRICKELL, Ernest / BROOKS, Clinton / CERF, Victor / DIFFIE, Whitfield / LANDAU, Susan / PETERSON, Jon / TREICHLER, John (2006): "Security implications…", cit., pág. 2. Con relación a los riesgos inherentes a la segunda opción, y los motivos por los que no resulta factible, ver: auts. y op. cits., págs. 11 y ss.

ofrecer sus servicios a los usuarios en España, circunstancia que determina que esta alternativa, además de inconveniente, sea de escasa relevancia práctica.

El otro gran obstáculo que se erige frente a la pretensión del Estado de mantener su capacidad para interceptor las comunicaciones es el de la encriptación. Durante la última década, la implementación de sistemas de encriptación "fuerte" para proteger comunicaciones de voz y datos se ha vuelto cada vez más común, minimizando la efectividad de los métodos tradicionales de intervención de comunicaciones[70]. El ejemplo más emblemático de ello está dado por la decisión adoptada en 2014 por WhatsApp -el servicio gratuito de mensajería para smartphones más importante a nivel global- de encriptar *por defecto* todas sus comunicaciones mediante un protocolo de encriptación "punto a punto" (*end-to-end*)[71], el cual oscurece los mensajes con una llave criptográfica a la que solo puede acceder el usuario y que nunca deja su equipo, impidiendo que puedan ser leídos por ningún tercero -*incluyendo a la propia compañía*. El resultado es encriptación prácticamente inexpugnable para los cientos de millones de celulares y tabletas que usan WhatsApp[72]. Y no solo esos: otras aplicaciones de gran popularidad, como iMessage de Apple o Telegram, también utilizan encriptación punto a punto que ni siquiera las propias compañías son capaces de penetrar[73].

El elemento en común que presentan los dos obstáculos reseñados precedentemente es que impiden o dificultan que la interceptación se concrete (o que acceda al contenido de las comunicaciones en formato legible) cuando los datos que forman parte de la misma se encuentran *en tránsito*, como ocurría hasta ahora conforme el modelo tradicional de intervención de comunicaciones. En cambio, cuando se recurre al *spyware* para llevar a cabo la interceptación, ésta tiene lugar en *los puntos de entrada o salida* de la comunicación (esto es, el móvil u ordenador usado por alguna de las personas involucradas en la conversación), por lo que captura los datos de audio, video y texto sin encriptar (toda vez que los datos se encriptan cuando están en tránsito, no cuando ingresan o egresan del dispositivo receptor o emisor)[74].

Vale señalar, por añadidura, que el uso de *spyware* para monitorear comunicaciones no se limita a las que se llevan a cabo a través de sistemas de comunicación, sino que también se puede utilizar dicha herramienta informática para capturar las que el objetivo esté manteniendo en forma presencial con otras personas. A tal efecto, el *software* estatal puede programarse para que, una vez introducido en el ordenador o el smartphone del sospechoso, active sin conocimiento de éste mecanismos de vigilancia como cámaras web o micrófonos. También se puede activar la cámara de un ordenador para que los investigadores observen lo

[70] Cfr. SWIRE, Peter (2011). "From real-time intercepts…", cit., pág. 1.
[71] Cfr. GASSER, Urs / GERTNER, Nancy / GOLDSMITH, Jack / LANDAU, Susan / NYE, Joseph / O'BRIEN, David R. / OLSEN, Matthew G. / RENAN, Daphna / SÁNCHEZ, Julian / SCHNEIER, Bruce / SCHWARTZOL, Larry / ZITTRAIN, Jonathan (2016): "Don't panic. Making progress in the 'going dark' debate", Berkman Center for Internet & Society, Harvard University, págs. 3/4 (énfasis añadido).
[72] Ver: GREENBERG, Andy (2014): "Whatsapp just switched on end-to-end encryption for hundreds of millions of users", en *Wired*, publicado el 18/11/2014, obtenido en: http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.
[73] Cfr. GELLER, Eric (2016): "A complete guide to the new 'Crypto Wars'", en *Daily Dot*, publicado el 26/4/2016 (actualizado el 5/5/2016), obtenido en: http://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/.
[74] Cfr. PELL, Stephanie K / SOGHOIAN, Christopher (2014): "Your secret Stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy", en *Harvard Journal of Law and Technology*, Vol. 28, N° 1, pág. 73 y nota § 380.

que sucede en un ámbito físico en un lugar determinado, o encender los micrófonos del ordenador o el teléfono móvil para escuchar las conversaciones que tengan lugar allí[75].

En este escenario, los recursos del Estado se han visto considerablemente ampliados a partir de la aparición del fenómeno tecnológico de la "Internet de las Cosas" ("*Internet of Things*" o IoT)[76], el cual comprende a una serie de dispositivos conectados a Internet que pueden ser explotados para la vigilancia (cámaras de seguridad, porteros electrónicos, dispositivos con control de voz como el Amazon Echo –"Alexa"- o los televisores "inteligentes" y hasta monitores de bebés) y han demostrado ser extremadamente vulnerables al hackeo.

El *spyware* resulta útil también para contrarrestar el recurso de los sospechosos a herramientas de anonimato tendientes a enmascarar, cuando se conectan a la Internet, sus verdaderas direcciones IP[77], cuyo conocimiento resulta clave para, en conjunción con otros datos, identificar la terminal informática utilizada para establecer cada conexión[78] y a partir de allí, a la persona responsable. Estas herramientas de anonimato (entre las que pueden destacarse a las "Redes Privadas Virtuales" - "*Virtual Private Networks*" o VPNs- y los sistemas TOR, I2P y Freenet) mantienen oculta la verdadera dirección IP de los usuarios redireccionando sus comunicaciones a través de múltiples estaciones o "nodos", encriptándolas y desencriptándolas repetidamente, hasta que los datos arriban a su destino final. De este modo, cada estación sólo "conoce" *una parte de la información* sobre la ruta seguida por los datos, por lo que el rastreo de los mismos en la Red se torna extremadamente difícil[79].

---

[75] Cfr. SALT, Marcos (2017), Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, Ad-Hoc, Buenos Aires, págs. 71/72.

[76] El concepto subyacente a la IoT es bastante sencillo: objetos equipados con identificadores de radio frecuencia (RFID) y sensores, capaces de comunicar información digital a otros sensores que la recolectan, a fin de crear redes de objetos "inteligentes" para contribuir a las necesidades de consumo, comercialización, salud, etc. La función de dichos objetos es recolectar y compartir información para volverse más eficientes o amigables para sus dueños. Los datos pueden ser almacenados localmente, compartidos mediante el WiFi o acumulados a través de aplicaciones de Internet que permitan el monitoreo de la información relevante (al respecto, ver: GUTHRIE FERGUSON, Andrew (2016): "The Internet of Things and the fourth amendment of effects", en *California Law Review*, Vol. 104, N° 4, pág. 812).

[77] La dirección IP es un código único que identifica a una determinada computadora conectada a la Internet ante el resto de los equipos con los que deseamos conectar. Así, cuando se enciende el equipo lo primero que hace es autenticarse en su Red a través de la dirección MAC de su tarjeta de red para obtener una IP pública, la cual, si es dinámica, una vez obtenida queda registrada durante el tiempo que dure la sesión. Esa IP pública es previamente obtenida por el proveedor de servicios de Internet (PSI) de las operadoras, a las que se les asignan determinados bloques de direcciones pertenecientes a cada región geográfica. No pueden existir en el mismo momento dos equipos informáticos conectados a Internet con la misma dirección IP, lo cual no impide que una misma dirección IP pueda ser utilizada por múltiples dispositivos informáticos en sus diversas conexiones a Internet, teniendo en cuenta el carácter finito y limitado del número de direcciones asignables a nivel global. De ahí la distinción entre dos grandes grupos de direcciones IP: las fijas o estáticas y las dinámicas, que se reparten entre los usuarios a los que provee de acceso a Internet una determinada empresa en función de una por cada sesión iniciada, reasignándose la misma a otro usuario una vez terminada la conexión (Cfr. ORTIZ PRADILLO, Juan Carlos (2015): "Fraude y anonimato en la red…, págs. 56/57).

[78] Cfr. ORTIZ PRADILLO, Juan Carlos (2015): "Fraude y anonimato en la red…", cit., pág. 58.

[79] Cfr. MONTIERI, Antonio / ACETO, Giuseppe / CIUONZO, Domenico / PESCAPÉ, Antonio (2018): "Anonymity services TOR, I2P, JonDonym: Classifying in the Dark (web)", en *IEEE Transactions on Dependable and Secure Computing*, obtenido en: https://www.researchgate.net/publication/322978661_Anonymity_Services_Tor_I2P_JonDonym_Classifying_in_the_Dark_Web, pág. 1.

La existencia de estas herramientas tecnológicas ha dado origen a lo que se conoce como la "red oscura" ("*dark web*") dentro de la Internet, en la que se encuentra el contenido online al que sólo puede accederse mediante un *software* de encriptación especializado como el TOR. En este sector de la Red existen páginas web especiales cuyos dominios terminan en ".onion", conocidas como "*hidden services*" ("servicios ocultos") cuyas ubicaciones reales son -en teoría- imposibles de localizar. Estos servicios ocultos ofrecen refugio a una intensa actividad ilícita cuya proliferación se ve favorecida por el anonimato que las mencionadas herramientas les ofrecen a los usuarios, en su mayoría centrada en derredor de "mercados oscuros" ("*dark markets*") como Silk Road, Alphabay o Hansa (todos ellos ya cerrados por las autoridades). Estos mercados online sacan provecho de los "servicios ocultos" para conectar a consumidores con proveedores, por lo general de bienes o servicios ilícitos. Pero los servicios de TOR también han sido utilizados para otros fines criminales, en especial la difusión e intercambio de explotación sexual infantil[80].

Frente a ello, en los EE.UU. las autoridades han recurrido al uso de spyware en el marco de "ataques de abrevadero" a fin de perseguir a los clientes de distintas páginas web ubicadas en la "red oscura" dedicadas al intercambio de imágenes de explotación sexual infantil, que ocultaban su localización e identidad mediante el uso de herramientas de anonimato. En ese orden de ideas, cobraron estado público tres operaciones del FBI bautizadas como "Operación Torpedo" (2012), "Operación Magneto" (2013) y "Operación Pacifier" (2015) que, combinadas, tuvieron como resultado el hackeo colectivo de miles de ordenadores en todo el mundo[81].

Por último, la existencia de software espía capaz de infiltrar teléfonos móviles, combinada con la generalización del uso de smartphones con GPS, le brinda al Estado la posibilidad de monitorear los movimientos de los ciudadanos en tiempo real y con un altísimo nivel de precisión (unos pocos metros). En esa dirección, vale señalar que, aunque es cierto que -en teoría- un sospechoso particularmente cuidadoso podría evitar ser rastreado ya sea optando por no llevar consigo el teléfono mientras delinque[82] o usando teléfonos prepagos que no puedan ser asociados con su persona, la realidad marca que la inmensa mayoría de la gente lleva encima *su propio teléfono* en todo momento.

Con relación a lo expuesto, es menester aclarar que la multiplicidad de usos posibles del *spyware* no importa necesariamente que deban desarrollarse programas específicos para cada uno de los usos reseñados. Ello, toda vez que -en especial a los efectos de la infiltración de teléfonos móviles- se han creado sofisticados programas espías denominados "amenazas combinadas" ("*blended threats*"), capaces de cumplir varias funciones de vigilancia en simultáneo. Si bien las más avanzadas de estas herramientas informáticas -como el "Smurf Suite" desarrollado conjuntamente por la NSA de los EE.UU. y el GCHQ británico- se encuentra fuera del alcance de las agencias policiales de la mayoría de los países (o pueden resultar

[80] Cfr. HERN, Alex (2017): "The dilemma of the dark web: Protecting neo-nazis and dissidents alike", en *The Guardian*, publicado el 23/8/2017, obtenido en: https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings. Con relación al uso de TOR para encubrir actividades de pornografía y explotación sexual infantil, ver: HENNESSEY, Susan (2017): "The elephant in the room…", cit.

[81] Cfr. AUCOIN, Kaleigh E. (2018): "The spider's parlour: Government malware on the dark web", *en Hastings Law Journal*, Vol 69, N° 5, pág. 1446.

[82] Opción que, dependiendo de la modalidad delictiva de que se trate, en la gran mayoría de los casos probablemente sea impracticable.

demasiado intrusivas en el contexto de una investigación criminal)[83], hoy en día éstas últimas pueden recurrir a spyware privados como el "Pegasus" de la empresa israelí NSO o el "FinFisher" de la firma Gamma Group; así como a otros programas similares disponibles en el floreciente mercado de soluciones informáticas privadas para las necesidades estatales en materia de ciberinvestigación, ciberseguridad y ciberespionaje.

4. Acceso remoto a sistemas informáticos

Aunque, a mi entender, todos los posibles usos de *spyware* para la investigación criminal están contemplados, directa o indirectamente, en las nuevas disposiciones introducidas en el Título VIII de la LEC a través de la LO 13/2015, el que surge más claramente es el del acceso remoto a los sistemas informáticos. Con relación a dicha medida, cabe tener presente que la misma puede concretarse de dos maneras. Por un lado, mediante lo que se conoce como un "registro extendido" ("*extended search*"), que consiste en acceder de modo remoto a los datos contenidos en un sistema que está conectado, a su vez, con otro que ha sido localizado e intervenido físicamente, bien sea como consecuencia de una entrada y registro o de otra manera. Por el otro, a partir de lo que se denomina un "registro remoto" ("*remote search*") propiamente dicho, que supone introducirse en un sistema informático no accesible en forma física o a través de un "registro extendido" a partir del uso de programas espía o *spyware*[84]. La LO 13/2015 a introducido disposiciones que regulan en forma expresa ambas modalidades, aunque nos centraremos en el segundo, por cuanto sólo éste constituye un verdadero supuesto de "hackeo legal"[85].

El "registro remoto" propiamente dicho se encuentra previsto en el nuevo artículo 588 septies de la LEC. Así, del propio texto del art. 588 septies (a)(1) se desprende que la norma habilita el acceso remoto a un sistema informático, ya sea recurriendo al nombre de usuario y contraseña reales del titular, obtenidos por cualquier otro medio (lícito), a los que se alude al referirse a "datos de identificación y códigos"; como al uso de programas espías o troyanos como los descriptos *supra*[86], cuya funcionalidad le permite a las autoridades no sólo echar mano a todo el contenido almacenado en (o accesible desde) el ordenador o dispositivo de que se trate[87], sino también monitorear en tiempo real la actividad que se realice con el mismo, todo ello sin conocimiento del usuario[88].

Se trata, pues, de una medida que además de ser completamente novedosa en el ámbito del proceso penal español, resulta muy controvertida debido al grado de intromisión que implica en la esfera de privacidad de las personas[89], derivado tanto del carácter clandestino del registro (es decir, de su desconocimiento por parte del afectado) como de la posibilidad de que el mismo se extienda en el tiempo[90]. En esa dirección, queda claro que recurso a programas espías autorizado por el ya citado art. 588 septies (a)(1) de la LEC constituye una injerencia sobre el

[83] Cfr. BOJARSKI, Kamil (2015): "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations", en *The European Review of Organized Crime*, Vol. 2, N° 2, pág. 26.
[84] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 5.
[85] El "registro extendido" ha quedado regulado en el art. 588 sexies (c)(3) de la LEC.
[86] Ver § 3.
[87] La posibilidad de extender el registro remoto a un segundo sistema conectado con el que ha sido accedido remotamente en primer término se encuentra prevista en el art. 588 septies (a)(3) de la LEC, que establece que "[c]*uando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro*".
[88] Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", cit., pág. 9.
[89] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 6.
[90] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 7.

derecho a la "intimidad personal" garantizado en el art. 18.1 de la Constitución Española (CE), que también establece en el art. 18.4 que "[l]*a ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

En orden a esta cuestión, resulta de gran interés el fallo dictado por el Tribunal Constitucional de Alemania (BVerfG) el 27 de febrero de 2008[91], en el que dicho tribunal creó o reconoció el derecho a la "confidencialidad e integridad de los sistemas de tecnología de la información", por considerar que las garantías de inviolabilidad del domicilio y el secreto de las comunicaciones previstos en la constitución de ese país (similares, en su formulación, a los consagrados en el art. 18 incs. 2 y 3 de la CE) no eran suficientes para proteger a los ciudadanos de la restricción potencial de sus libertades derivada de la facultad estatal de acceder remotamente a sus ordenadores[92]. En esa dirección, entendió que este nuevo derecho protege el interés del usuario de un sistema de tecnología de la información en que se garantice la confidencialidad de los datos creados, procesados y almacenados en el mismo, cuya integridad es violada cuando se accede al mismo de modo tal que terceros puedan controlar su performance, funciones y contenidos[93].

Si bien la sentencia del BVerfG no estableció un derecho absoluto a la "confidencialidad e integridad de los sistemas de tecnología de la información", sólo admite su restricción cuando existan datos fácticos de un concreto peligro para un bien jurídico "especialmente destacable" (el cuerpo, la vida y la libertad de la persona o semejantes bienes de la comunidad, cuya amenaza afecte a los Fundamentos o la propia existencia del Estado o de las personas)[94]. Aunque el tribunal flexibilizó un tanto este requisito al disponer que no se demanda la demostración de un alto grado de probabilidad de que el peligro se materialice en el futuro cercano para validar la injerencia[95], lo cierto es que el estándar establecido por el BVerfG parece excesivamente riguroso, ya que excede lo admitido para restringir los derechos a la inviolabilidad del domicilio y el secreto de las comunicaciones que el tribunal combinó para dar origen al nuevo derecho a la "confidencialidad e integridad de los sistemas de tecnología de la información".

En efecto, parece evidente que en el contexto tecnológico actual -y en especial en el que habrá de imperar en el futuro cercano- el criterio sentado en el fallo del BVerfG resulta inaplicable, en la medida en que sólo permite el uso de *spyware* en un universo reducidísimo de casos[96], dejando inerme al Estado frente a delincuentes u organizaciones criminales que hagan uso de las variadas herramientas tecnológicas anti forenses disponibles para impedir que las autoridades accedan a la evidencia digital de algún otro modo. Y ello, en contraposición con la propia jurisprudencia del referido tribunal, que ha puesto de manifiesto en repetidas ocasiones la necesidad ineludible de lograr una persecución eficaz de los delitos, enfatizando el interés público en llegar a la verdad en el proceso penal, y señalando que el esclarecimiento –

[91] BVerfG, NJW 2008, 822. El fallo en cuestión se dictó con relación a la constitucionalidad de una disposición que habilitaba el acceso remoto a un sistema informático en términos similares a los del art. 588 septies (a)(1) de la LEC.

[92] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 110. En mayor detalle, sobre los argumentos esgrimidos por el BVerFG para fundar su postura sobre la insuficiencia de las garantías de inviolabilidad del domicilio y el secreto de las comunicaciones para ofrecer una protección suficiente, ver aut. y ops. cits., págs. 116/119.

[93] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 120.

[94] Cfr. ORTIZ PRADILLO, Juan Carlos: "El 'remote forensic software'…", cit., pág. 5.

[95] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 121.

[96] El que hasta podría excluir, dependiendo de la interpretación, a la difusión de imágenes de explotación sexual infantil, en la medida en que no se demuestre previamente que hay menores en riesgo inminente.

especialmente de delitos graves– constituye un cometido esencial del estado de Derecho de cualquier entidad pública[97].

Apartándose del criterio sostenido por el VBerfG, el legislador español dispuso en el citado art. 588 septies (a)(1) de la LEC los supuestos en que la medida de acceso remoto mediante *spyware* puede autorizarse. En tal contexto, la decisión de legitimar el uso de *spyware* para perseguir "[d]*elitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación*" ha generado las mayores críticas por parte de la doctrina, como por ejemplo la de BUENO DE MATA, que considera que la misma deja "una puerta peligrosamente abierta", que en su opinión se debería eliminar para evitar que el uso de esta herramienta de manera analógica quede librada a la discrecionalidad del juzgador[98]. En igual sentido, VEGAS TORRES argumenta que una medida tan invasiva de la privacidad solamente está justificada para la investigación de delitos muy graves, recordando que en otros países su incorporación ha sido objeto de fuertes debates y se ha llevado a cabo con sujeción a límites más estrictos[99]. Por su parte, RUBIO ALAMILLO objeta que la reforma, al dejar sujeta a "*…vagos criterios del medio a través del cual se comete el delito investigado*" la posibilidad de suspender algo tan importante como los derechos fundamentales, posibilite que se la autorice para la investigación de delitos considerados *menores*[100].

En dicho orden de ideas, BACHMAIER WINTER apunta que, aunque el legislador haya indicado que la disposición en análisis es un elemento para valorar el interés público, lo cierto es que el hecho de que un delito concreto se cometa en el entorno digital en realidad no afecta al interés público, sino que se vincula con la mayor dificultad de esclarecer el delito en caso de que no se adopten medidas de investigación tecnológica. La circunstancia de que el delito se haya cometido a través de sistemas informáticos no justifica automáticamente la adopción de una medida de investigación telemática, y tampoco la medida del registro remoto de ordenadores o dispositivos, pero sí abre la puerta a que la medida se acuerde, incluso aunque el delito no sea calificado como grave por razón de la pena[101]. Para la autora citada, la respuesta al interrogante sobre por qué el legislador ha autorizado el uso de una medida tan invasiva para investigar delitos no tan graves puede encontrarse en la valoración de su *necesidad*. Ello, toda vez que, por sus peculiares características, la inmensa mayoría de los delitos informáticos no podrán descubrirse –y por tanto quedarán impunes– a menos que se autoricen medidas de investigación telemática. En tal contexto, el interés público deriva precisamente del fin legítimo que es evitar una tal impunidad generalizada, que en última instancia llevaría a que Internet se convirtiese en un territorio al margen de la ley. Los peligros a los que se enfrenta el "ciudadano global" en semejante escenario justificarían ese planteamiento[102].

En sustento de este estándar más flexible para la imposición de la medida en trato, vale tener presente que el art. 8.2 del CEDH admite la injerencia sobre los derechos cuando la medida sea necesaria para "*…la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección*

[97] Sentencias del BVerfG 29, 183; 77, 65; 80, 367; y 100, 313.
[98] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.
[99] Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", cit., pág. 9.
[100] Cfr. RUBIO ALAMILLO, Javier (2015): "La informática en la reforma…", cit. (énfasis en el original).
[101] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 16.
[102] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 23. Al respecto, la autora recuerda que en relación con intervenciones telefónicas el tribunal Constitucional ya ha determinado que el requisito de la proporcionalidad no exige necesariamente que el delito investigado sea grave por razón de la pena, puesto que la gravedad del mismo puede derivar de otros elementos, al margen de la sanción atribuida (Ibídem, pág. 23, nota § 42, con cita de las SSTC 299/2000, de 11 de diciembre de 2000, y la STC 82/2002, de 22 de abril).

de los derechos y libertades de los demás". En línea con ello, la prevención del delito y la defensa del orden, considerados como pilares de toda política criminal en las democracias modernas, son contemplados en el convenio con la amplitud justa para conferir un notable margen de apreciación nacional a los países. Es por tal motivo que -como apunta RUIZ LEGASPI- no resulte frecuente que en la jurisprudencia del TEDH se rechace la legitimidad de una medida adoptada en el curso de una investigación criminal[103]. De hecho, el referido tribunal suele conformarse, para admitir la legitimidad de medidas restrictivas de derechos, con la invocación genérica del concepto de "defensa del orden", el cual puede subsumir de un modo u otro casi todas las demás finalidades legítimas previstas en el convenio, y a las que en mayor o menor medida responde siempre la actuación de los poderes públicos, especialmente en el ámbito criminal[104].

Lo expuesto no significa, sin embargo, que el juez deba necesariamente acordar un registro remoto de ordenadores a través de *spyware*, en los casos en que la ley lo autoriza por haberse cometido el delito a través de sistemas informáticos y existan sospechas fundadas acerca de la comisión del mismo. Por el contrario, es preciso que antes de autorizarlo pondere todos los elementos para apreciar si la medida, en el caso concreto, cumple con el principio de proporcionalidad[105].

Si bien las disposiciones en trato no lo establecen expresamente, entiendo que también autorizan el acceso remoto al sistema mediante *spyware* ya sea para obtener los "datos de identificación y códigos" necesarios para ingresar a otros servidores conectados con el sistema original (por ejemplo, a fin de recuperar la evidencia que el sospechoso pueda haber almacenado "en la nube") o las llaves criptográficas requeridas para tornar legible la información encriptada; puntualmente a partir del recurso a un programa "*keylogger*".

A mi juicio, abona esta conclusión lo dispuesto en el art. 588 septies (c), que prevé que la medida puede tener "*…una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses*". Ello, toda vez que si lo que se pretende autorizar mediante las normas en estudio es tan solo la obtención de los datos almacenados en un sistema informático en un momento dado, el plazo parece excesivo, pues una vez instalado el *spyware* y concretada la intrusión, la mencionada información digital puede "registrarse" por medio de una "imagen" forense en cuestión de minutos u horas, dependiendo del grado de "latencia" (velocidad) de la conexión. En tal contexto, mantener el *spyware* después de haber clonado los datos especificados en la orden judicial importaría convertir la medida en una observación o interceptación del entorno digital de un sujeto por un plazo determinado. Si esto es lo que en efecto ha querido permitir el legislador, no se trataría tanto del registro de un ordenador realizado a distancia para evitar el conocimiento del titular, sino más bien de una observación de su entorno digital a través del hackeo de su ordenador[106]. Si no lo es, entonces una vez concretado el acceso y el registro con la preservación de los datos, la medida debería cesar, puesto que el objetivo para el que se autorizó ya se ha cumplido. lo cual debería llevar a que quienes ejecutan la medida procedieran a desinstalar o desactivar el *spyware*[107].

Por añadidura, parece evidente que la regulación de una medida en términos parecidos -en orden a su alcance temporal- a los de la interceptación de las comunicaciones no es casual, sino que obedece a la intención de permitir el monitoreo del entorno digital del objetivo por un

[103] Cfr. RUIZ LEGAZPI, Ana (2014): "Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (incoming de Emule) en la STC 173/2011", en *Revista Española de Derecho Constitucional*, N° 100, pág. 370.
[104] Cfr. RUIZ LEGAZPI, Ana (2014): "Derecho a la intimidad y obtención de pruebas", cit., pág. 371.
[105] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 24.
[106] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 18.
[107] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., págs. 17/18.

período limitado de tiempo, por ejemplo para obtener la información necesaria (nombre de usuario y contraseñas) para habilitar el acceso a la evidencia digital almacenada en otro sistema conectado con aquél -conforme lo previsto en el art. 588 septies (a)(3)- o a fin de desencriptar datos almacenados en el primero. La expresa referencia a los "datos de identificación y códigos" en el primer párrafo del art. 588 septies (a)(1) y la alusión al "el software mediante el que se ejecutará el *control* de la información"[108] en el art. 588 septies (a)(2)(b) también refuerzan, a mi modo de ver, la referida conclusión.

En cuanto al modo en que debe ejecutarse la medida, el art. 588 septies (a)(2) establece una serie de requisitos a cumplir por la orden judicial que autoriza el registro -sin perjuicio de las disposiciones comunes a todas las medidas incorporadas por la LO 13/2015 previstas en el art. 588 bis (a) y subsiguientes de la LEC-, entre las que se encuentra la de especificar a qué dispositivos o sistemas se dirige la medida. Al respecto, BACHMAIER WINTER apunta que lo que no se regula es qué ordenadores pueden interceptarse a distancia, ni los casos y condiciones en que podría someterse a registro remoto el ordenador de un tercero. En opinión de la autora citada, ello genera dos interrogantes importantes en la práctica. Primero, si el registro remoto solo puede acordarse para acceder al ordenador del sospechoso o si puede también autorizarse para registrar el ordenador que, aun siendo de otro sujeto, posiblemente está siendo utilizado por el sospechoso para almacenar o para comunicar. Y segundo, si puede autorizarse el registro remoto del ordenador de un tercero, aunque no esté siendo utilizado por el sospechoso, pero en el cual pueden existir datos relevantes para el esclarecimiento del delito[109].

En orden a esta cuestión, BACHMAIER WINTER considera aplicable, *mutatis mutandi*, al registro remoto de equipos informáticos la regla prevista en el art. 588 bis (h) de la LEC, que habilita la interceptación de comunicaciones que afecten a terceras personas, por considerar que el registro remoto de un ordenador a través de la instalación de *software* implica siempre una interceptación de las comunicaciones. Entiende que ello es así porque se trata de una medida que utiliza un proceso de comunicación electrónica como vía para acceder al contenido de un equipo informático. Argumenta que, aunque el proceso comunicativo no es el fin de esta medida –lo sería en el caso de una interceptación de las comunicaciones del ordenador en tiempo real–, sí implica una intervención en el proceso comunicativo, aunque solo sea para instalar el *spyware* en el equipo informático objeto del registro. Podría decirse que es una medida que implica una interceptación de las comunicaciones, aunque el proceso de interceptación en sí no afecte al derecho al secreto de las comunicaciones[110].

Otros autores, sin embargo, objetan la premisa en la que buscó apoyo la autora citada para sostener la posibilidad de aplicar analógicamente el art. 588 bis (h) de la LEC al registro remoto. Así, ABEL y SCHAFER señalan que la circunstancia de que, para poder introducirse en el sistema, el troyano requiera que en algún momento el sospechoso se encuentre *online* y comunicándose, no asimila la medida a una interceptación de comunicaciones, del mismo modo en que el secuestro de un teléfono móvil durante el registro físico de una vivienda no convierte al allanamiento en una interceptación de las comunicaciones[111]. En igual sentido, ORTIZ PRADILLO señala que el secreto de las comunicaciones no se pone en juego cuando mediante el registro online de un equipo informático lo que se pretende no es "interceptar" una comunicación o tomar conocimiento de su contenido sino "acceder" -a través de las vías de comunicación existentes- al interior de un equipo informático con el objetivo de inspeccionar y/o remitir el

[108] Énfasis añadido.
[109] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 11.
[110] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 12.
[111] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 113.

contenido del mismo[112]. Esto es: cuando la comunicación no es el objetivo de la medida, sino el medio para concretarla.

Si bien coincido con los autores citados en último término en punto a que el acceso remoto a un ordenador a través de Internet no puede ser asimilado a la interceptación de una comunicación (aunque instrumentalice una comunicación para poder llevarse a cabo), entiendo que ello no obsta a que pueda considerarse permitida la concreción de la referida medida con relación a un equipo informático no perteneciente al sospechoso. Y ello, por varios motivos. En primer lugar, por cuanto en la investigación de varias modalidades de ciberdelitos puede ignorarse si el equipo o sistema informático que se sabe que puede contener evidencia relevante pertenece en realidad al sospechoso o a un tercero cuyo ordenador está siendo controlado remotamente por aquél[113]; como así tampoco conocer ese dato sin revelar la existencia de la investigación y, por ende, comprometer su éxito. De igual manera, si se utilizan herramientas de anonimato como el sistema TOR para conectarse con una página web ubicada en la "red oscura" y -por ejemplo- descargar o distribuir imágenes de explotación sexual infantil, recién va a poder saberse quién es el sospechoso -o si el ordenador le pertenece a él o no- una vez que se haya concretado la intrusión de su ordenador.

Por otro lado, el art. 588 septies (a)(2) de la LEC dispone que la orden judicial que autorice el registro remoto debe determinar el alcance de la medida, la forma de acceso y el *software* a utilizar. En lo tocante al posible *alcance* de la medida, una cuestión que se suscita es si podría comprender también la interceptación en tiempo real de telecomunicaciones. Al respecto, se apunta que la alusión al examen del "contenido" del sistema o equipo objeto de la medida en el art. 588 septies (a)(1) pareciera excluir dicha posibilidad. Es cierto que para las comunicaciones electrónicas escritas esa distinción no tiene mucha relevancia, pues una vez enviadas –abiertas o no, leídas o no–, si no se eliminan serán almacenadas en el dispositivo y serían accesibles a través del registro remoto del mismo. En efecto, en los términos del legislador español, los correos electrónicos almacenados pasan a formar parte del "contenido" del dispositivo[114] y su obtención en esos casos no importa un monitoreo *en tiempo real*.

En realidad, a partir de la LO 13/2015 esta forma de monitoreo se encuentra regulada en los arts. 588 ter (a) y 588 ter (b)(1) de la LEC, en cuanto habilitan la interceptación de comunicaciones "telemáticas" interviniendo "los terminales o medios de comunicación", entre los que deben considerarse comprendidos, evidentemente, a todos los sistemas informáticos que permitan desarrollar una comunicación telemática (ordenadores, tabletas, smartphones, etc.)[115]. Circunstancia que abona la opinión de BACHMAIER WINTER en punto a que, al regular el registro remoto de equipos informáticos, la intención del legislador no ha sido cubrir también la interceptación en tiempo real de las telecomunicaciones[116].

Sin embargo, la cuestión se torna algo más difusa si se la analiza con relación al supuesto de uso de la medida de registro remoto ya no para obtener únicamente los datos almacenados en un equipo informático en un momento dado (esto es, como si se tomara una fotografía del "contenido" del equipo), sino para monitorear el entorno virtual a través del uso de un programa *keylogger*. Ello, toda vez que, en este caso, el referido programa va ir recogiendo el

[112] Cfr. ORTIZ PRADILLO, Juan Carlos (2009): "El 'remote forensic software'…", cit., pág. 5.
[113] Esto es, si se trata de un "bot" u "ordenador zombie", que ha sido infiltrado mediante la introducción de un programa malicioso que le permite al sospechoso controlar el equipo en forma remota y utilizarlo sin conocimiento de su propietario. Por ejemplo, para enviar SPAM o participar en ataques de "denegación distribuida de servicio" ("*distributed denial of service*" o DDOS).
[114] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 14.
[115] En más detalle, sobre esta cuestión, ver *Infra* § 5.
[116] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 15.

contenido de las comunicaciones escritas (mensajes en grupos de chats, *mails*, etc.) a medida que el usuario las escribe. En la jurisprudencia de los EE.UU., esta cuestión fue objeto de análisis en el caso "Scarfo"[117], en el que la fiscalía argumentó exitosamente que la captación de todo lo tecleado en un ordenador no constituía una interceptación de las comunicaciones electrónicas, debido a que el programa *keylogger* utilizado estaba programado para no funcionar cuando el modem estuviese encendido[118].

La descripción, en la orden judicial, del modo en que funciona el *software* empleado para concretar la medida resulta esencial para permitir un análisis posterior sobre la proporcionalidad de la misma y la legitimidad de la injerencia concretada en los derechos del sujeto pasivo del registro. En ese orden de ideas, RUBIO ALAMILLO califica como "un escollo muy importante" la indefinición, en el texto legal, del tipo de programas informáticos que se van a utilizar para espiar a los ciudadanos[119], de dónde se van a poner los límites a las acciones que pueden realizar dichos programas y de qué profesionales van a auditar de forma externa el código fuente de estos programas para verificar que efectivamente no se extralimitan en sus funciones, aspecto que a su entender genera una inseguridad jurídica inaceptable[120].

No comparto esta crítica. Ello, toda vez que, en primer lugar, la constante evolución de la tecnología torna imposible que en una norma de carácter procesal se pueda determinar, con un mínimo de precisión, el modo en que debería funcionar el programa informático con el que se concreta la medida de acceso remoto. Siendo que, además, no resulta conveniente fijar los límites a las acciones que habrá de realizar el *spyware* de modo general, sino atendiendo a las circunstancias particulares de cada caso y en función del alcance de la medida autorizada por el juez. Por ende, el modo en que se regula la cuestión en el art. 588 septies (a)(2)(b) resulta más eficaz, en cuanto manda a precisar, en cada caso concreto, como habrá de funcionar el programa efectivamente empleado. En tal sentido, lo que corresponderá será verificar que el *spyware* garantice que la recolección de datos se lleve a cabo minimizando el impacto sobre el entorno informático en el que corre y que permita el registro de todas las acciones (y modificaciones) que ejecuta dentro del sistema infiltrado, para que con posterioridad pueda verificarse que no se afectó la integridad y confiabilidad de la evidencia obtenida. Circunstancia que, vale aclararlo, se encuentra prevista en el art. 588 septies (a)(2)(e) de la LEC.

A diferencia de lo que ocurre con la interceptación de comunicaciones y el seguimiento y localización, que expresamente prevén que el plazo de duración de la medida empieza a contarse a partir de la fecha de la autorización judicial, el art. 588 septies (c) de la LEC no define el *dies a quo* del término de prolongación de la medida de acceso remoto al sistema informático. Ante la diferente regulación de uno y otro supuesto por parte del legislador, cabe preguntarse si el plazo de un mes (prorrogable hasta tres meses) establecido en la disposición en trato comienza a correr desde que se autoriza la medida o desde que la misma comienza a hacerse efectiva.

Al respecto, VEGAS TORRES considera que debe aplicarse el mismo criterio para todas las medidas introducidas por la LO 13/2015 (es decir, que los plazos empiecen a correr a partir de la

---

[117] *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 (Corte Federal de Apelaciones del Distrito de New Jersey, 26 de diciembre de 2001).

[118] Cfr. CARRELL, Nathan E. (2002): "Spying on the mob: United States v. Scarfo – A constitutional analysis", en *Journal of Law, Technology & Policy*", Vol. 2002, N° 1, pág. 209.

[119] El autor destaca, a ese respecto, que en la práctica, las posibilidades que ofrecen el uso de este tipo de sistemas son muy amplias, inclusive el envío y recepción de archivos ilícitos a través de una *backdoor* sin que el sospechoso se percate, tal y como indica el nuevo artículo 282 bis, apartado 6, de tal forma que luego podrían ser utilizados judicialmente en su contra.

[120] Cfr. RUBIO ALAMILLO, Javier (2015): "La informática en la reforma…", cit.

fecha de la autorización judicial), dato que se trata de una tesitura que ya ha sido ratificada por la jurisprudencia[121]. Coincide con esta opinión CASANOVA MARTÍ, quién recuerda que en esa dirección se pronunció el TC en su sentencia N° 26/2006, de 30 de enero[122], decantándose por la primera opción basándose en el principio de interpretación de la legalidad en el sentido más favorable a la efectividad de los derechos fundamentales, lo que llevaría a la lectura más garantista desde la perspectiva del secreto de las comunicaciones[123].

En sentido opuesto, BACHMAIER WINTER recuerda que en ocasiones puede transcurrir cierto tiempo hasta que logra instalarse el *software* en el equipo que se pretende registrar, o que, una vez instalado, pasa un tiempo hasta que está operativo. Esta circunstancia no es problemática si la puesta en funcionamiento se demora más de un mes, toda vez que puede solicitarse prórroga al juez explicando los motivos por los que todavía no se ha podido acceder a los datos contenidos en el equipo que es objetivo de la medida[124]; pero si lo es si transcurren más de tres meses desde que se autoriza el registro remoto y, por motivos técnicos, el *software* no está operativo y no se ha podido acceder a los datos (como podría ocurrir, por ejemplo, si en ese lapso el sospechoso no hubiese abierto el ordenador o activado aquellos concretos programas que permiten al *spyware* entrar en el sistema). La pregunta es si, en tal caso, la autorización debe cesar o puede extenderse más allá del tope de tres meses establecido en la norma[125]. En tal contexto, la autora citada entiende que, debido a sus singulares características, la duración del registro remoto de equipos informáticos debería establecerse tomando como punto de partida el momento en que el equipo en cuestión resulta accesible, esto es, una vez instalado y operativo el *software*[126].

Considero, por mi parte, que corresponde interpretar que en cuanto atañe a la medida de acceso remoto a los sistemas informáticos, el plazo de duración de la medida empieza a correr a partir de que el programa espía comienza a funcionar. Y ello, por dos motivos. En primer lugar, dando pleno efecto a la intención del legislador conforme se desprende del tenor literal de las disposiciones en estudio. Ello importa reconocer que si en una misma ley (la LO 13/2015), el legislador incorporó simultáneamente varias medidas restrictivas de derechos fundamentales y las reglamentó en forma *diferente* en cuanto al *dies a quo* (precisando respecto de unas que el plazo de duración comienza a correr a partir de la autorización judicial, y omitiendo hacerlo en otra), no cabe más que concluir que ello obedece a que pretende que funcionen de modo distinto, no igual. Tanto más cuando existe un motivo práctico que otorga sustento a dicha distinción, que es la posibilidad de que la puesta en funcionamiento del spyware demore más tiempo del previsto como tope de duración de la medida en el art. 588 septies (c) de la LEC.

En segundo lugar, cabe señalar que la interpretación que aquí se propicia no redunda en una injerencia más intensa sobre los derechos fundamentales del ciudadano objeto de la medida, toda vez que, en realidad, dicha injerencia no empieza a producirse hasta que el programa espía comienza a funcionar. Y ello, incluso tomando como referencia al derecho a la "integridad y confidencialidad de los sistemas de tecnología de las comunicaciones" creado por el BVerfG. En

[121] Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", cit., pág. 18 (Con cita de las SSTS del 11 de enero de 2017, de 25 de marzo de 2015, y del 1 de octubre de 2013, entre otras).
[122] STC, 2ª, 30.1.2006 (BOE 51, 1.3.2006, MP: Guillermo Jiménez Sánchez).
[123] Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit.
[124] Aunque en tal caso, se ha consumido sin obtener ninguna evidencia un tercio del tiempo autorizado por la ley procesal para el cumplimiento de la medida.
[125] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 18. Aunque en principio, esta posibilidad estaría vedada por lo establecido en el art. 588 bis (e)(3), que dispone que una vez "[t]*ranscurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos*".
[126] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 18.

efecto, se aprecia que el derecho a la intimidad (incluyendo el secreto de las comunicaciones) no se ve afectado hasta que el *spyware* empieza a captar y transmitir los datos contenidos en el sistema, lo cual no ocurre cuando no está en funcionamiento. De igual manera, la *integridad* del referido sistema tampoco es vulnerada hasta que el programa se ejecuta, sin importar si ya se encuentra, o no, dentro de ese sistema. Cabe tener presente, en tal sentido, que cuando el *spyware* es recibido por el sospechoso en su ordenador o teléfono móvil, no difiere de cualquier otro contenido informático: mientras se encuentra inactivo, no es más que información digital, como lo sería una fotografía o un archivo de texto. Recién cuando el programa se ejecuta pasa a tener la capacidad para modificar el entorno digital que lo rodea y, de esa manera, comprometer la integridad del sistema informático invadido.

5. Monitoreo de comunicaciones

Como ya se señalara al comienzo del presente trabajo[127], la LO 13/2015 vino a llenar un vacío legal en la LEC que había sido especialmente problemático en todo lo tocante a la interceptación de las comunicaciones electrónicas, dado que el art. 579 de la referida norma sólo amparaba, *estricto sensu*, el monitoreo de "*…la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros*", cuestión que derivó en sendas sentencias adversas respecto de España por parte del TEDH en orden a la defectuosa protección del secreto de las comunicaciones. En cambio, a partir de la reforma, el art. 588 ter (a) de la LEC autoriza en forma expresa "*…la interceptación de las comunicaciones telefónicas y telemáticas*" en los mismos supuestos comprendidos por el art. 579 (1) de la misma norma; a los que el legislador le adicionó la persecución de "*…delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*".

Como explica BUENO DE MATA, el texto actual de la LEC ampara la interceptación de cualquier aplicación ofrecida por un smartphone, incluyendo los nuevos tipos de mensajería derivadas de aplicaciones como WhatsApp o Telegram, confiriendo así sustantividad propia a otras formas de comunicación telemática que previamente carecían de tratamiento normativo en la normativa procesal[128]. Ahora bien: teniendo en cuenta lo expresado *Supra*[129] en orden al modo en que las referidas aplicaciones (dotadas de encriptación "punto a punto") y los sistemas VoIP como Skype o Facetime ponen en jaque la "interceptabilidad técnica" de las comunicaciones telemáticas, surge el interrogante de si se encuentra legalmente autorizada, o no, la utilización de *spyware* estatal para salvaguardar las facultades que la ley le otorga. Ello, toda vez que a diferencia del art. 588 septies (a)(1), que regula el acceso remoto a los equipos o sistemas informáticos, las normas vinculadas a la interceptación de las comunicaciones telefónicas o telemáticas no hacen alusión expresa a la posibilidad de llevar a cabo dicha interceptación por medio de la "instalación de un software".

Entiendo que, a pesar de la omisión señalada en el párrafo precedente, el texto legal permite concluir que la respuesta debe ser afirmativa. En esa dirección, vale destacar que al definir el "ámbito" u objeto de la intervención, el art. 588 ter (b)(1) alude a "[l]*os terminales o medios de*

[127] Ver *Supra*, § 1.
[128] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.
[129] § 3.

comunicación" utilizados por aquél[130]. Esto es: a los equipos (*smartphone*, ordenador) que el sospechoso usa para comunicarse. En igual sentido, en el art. 588 ter (b)(2) se establece que la intervención "*…podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario*", mientras que en el último párrafo del art. 588 ter (c) se autoriza a intervenir el terminal o medio de comunicación telemática de un tercero "*…cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular*", supuesto vinculado a la instrumentalización de ordenadores ajenos mediante programas maliciosos, convirtiéndolos en equipos "zombies" o "bots". Por último, el art. 588 ter (d)(1)(4) de la LEC prevé que la solicitud de autorización judicial debe comprender "*…la identificación del número de abonado, del terminal o de la etiqueta técnica*"[131].

Lo que se desprende del texto de las disposiciones reseñadas es que, a diferencia de lo que ocurría en el pasado con las intervenciones telefónicas, en las que se identificaba el objetivo de la interceptación referenciando la línea telefónica cuyo titular era el sujeto investigado, en la LO 13/2015 el legislador -con buen criterio- ha optado por poner el énfasis *en los dispositivos* mediante los cuales se lleva a cabo la comunicación, permitiendo de ese modo que ésta medida se adapte a las características del nuevo escenario tecnológico en materia de comunicaciones telemáticas.

Así las cosas, parece evidente que la circunstancia de que no se haya precisado en la normativa el *método* técnico mediante el cual ha de llevarse a cabo la interceptación *del terminal o medio de comunicación* -conforme la autorización expresamente establecida en la LEC- no obsta a que pueda recurrirse al *spyware* para lograrlo. Ello, toda vez que se trata, a fin de cuentas, de una herramienta técnica especialmente apta para concretar la medida en los términos previstos en la regulación procesal (esto es: tomando como objetivo al terminal o dispositivo utilizado para la comunicación), de modo tal que la legitimidad de su uso en cada caso concreto dependerá del resultado del análisis de la capacidad del *software* para cumplir con los fines y límites establecidos en la autorización judicial.

La circunstancia de que la herramienta técnica sea un programa informático no violenta lo dispuesto en el art. 18.4 de la CE, desde que en realidad no se está concretando, a través del *spyware*, una intrusión nueva o más intensa respecto de los derechos de los ciudadanos que la que entraña la interceptación de las comunicaciones por los medios tradicionales, sino únicamente extender esta facultad ya asignada legalmente al Estado a las nuevas modalidades de comunicación (por ejemplo, los servicios de mensajería encriptada). Al respecto, resulta de aplicación lo señalado por el TS en su sentencia N° 1563/2004, de 24 de enero[132], en la que dejó sentado que el juez no tiene obligación de precisar los sistemas técnicos o los medios electrónicos a emplear por la Policía Judicial en la ejecución de la medida, por ser cuestiones ajenas y propias de los especialistas policiales, criterio ratificado posteriormente en la sentencia Nº 722/2012, de 2 de octubre[133], oportunidad en la que se explicó que "*…cuando el*

[130] Aunque el art. 588 ter (b), anteúltimo párrafo, autoriza también a intervenir "*…los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad*", como asimismo el de terceras personas cuando "*…exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información*" (art. 588 ter. (c)(1)) o "*…titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad*" (art. 588 ter. (c)(2)).
[131] Énfasis añadido.
[132] STS, 2a en lo penal, 24.1.2005 (MP: Diego Antonio Ramos Gancedo).
[133] STS, 2a en lo penal, 2.10.2012 (MP: Cándido Conde-Pumpido Touron).

Juez ordena una intervención telefónica no impone la utilización de ningún sistema, sino que autoriza los más avanzados o los que en un momento dado utilice la policía judicial, siempre que ofrezcan plenas garantías".

La interpretación que aquí se propicia encuentra sustento, por añadidura, en un argumento -si se quiere- teleológico. Es decir, uno que atiende al propósito que alentó la incorporación de las disposiciones en trato en la LEC a través de la LO 13/2015, que no fue otro que adaptar la normativa procesal a la realidad tecnológica imperante. Con esa finalidad en mente, se dificulta sostener que la interceptación de comunicaciones haya sido regulada por el legislador de un modo que invalide el *único método disponible* para acceder a las que se llevan a cabo bajo el amparo de la encriptación, que al día de hoy constituyen una porción cada vez más importante (tanto en términos de volumen como de relevancia) de las comunicaciones interpersonales. En especial, toda vez que ello importaría afirmar que: a) una reforma tendiente a actualizar la legislación procesal fue pensada para ser obsoleta desde su misma sanción, al excluir la posibilidad de intervenir un amplio rango de las comunicaciones de la población; y b) que de ese modo, se deja al Estado inerme frente a una de las principales herramientas con las que cuentan las principales organizaciones criminales que operan en Europa y el mundo (incluyendo a las responsables de catastróficos ataques terroristas durante las últimas dos décadas).

En orden a este último punto, vale hacer mención a la operación concretada por las policías de Francia y los Países Bajos junto con Europol y Eurojust contra la red EncroChat, especializada en ofrecer herramientas de encriptación de las comunicaciones cuyo abuso -según explicó la propia Europol en el comunicado de prensa publicado en relación con dicha operación[134]- ha sido uno de los factores claves en la actividad de una serie de organizaciones criminales en los países europeos durante los últimos años, a punto de convertirse en uno de "*…los desafíos de seguridad más acuciantes para las autoridades judiciales y de cumplimiento de la ley*". Aunque EncroChat no era la única compañía ofreciendo esta clase de productos, especialmente diseñados para favorecer la impunidad de los criminales[135], si ostentaba una posición dominante en ese rubro en el mercado de la criminalidad organizada en Europa[136], garantizando "perfecto anonimato" a partir de la compra de sus teléfonos y la suscripción de los servicios de dicha firma[137]. En tal contexto, el hackeo, por parte de las autoridades francesas, de los

[134] Ver: Europol (2020): "Dismantling of an encryted network sends shockwaves through organized crime groups across Europe", publicado el 2/7/2020, obtenido en: https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

[135] Además, de EncroChat, surgieron en los últimos años MPC (creada, de hecho, por una organización criminal dedicada al narcotráfico en Escocia), Phantom Secure (cerrada por el FBI en los EE.UU.) y Omerta, que ya se está publicitando como la sucesora de EncroChat a partir del ataque sufrido por ésta última (ver: Cox, Joseph (2020): "How police secretly took over a global pone network for organized crime", en *Motherboard. Tech by VICE*, publicado el 2/7/2020, obtenido en: https://www.vice.com/en_us/article/3aza95/how-police-took-over-encrochat-hacked).

[136] Cfr. Cox, Joseph (2020): "How police secretly took over a global pone network for organized crime", cit.

[137] A tal efecto, EncroChat comercializa los equipos de un modo completamente anónimo, sin registro de la identidad de los adquirentes y sin asociar la tarjeta SIM con la cuenta del usuario. Asimismo, los equipos propiamente dichos son modificados para servir únicamente para el envío de mensajes (encriptados), removiendo los elementos que facilitan el hackeo e interceptación (cámara, micrófono, GPS y puerto USB). Por añadidura, están programados para borrar los mensajes una vez recibidos por el destinatario y contienen funciones como la eliminación inmediata de todo su contenido si se producen

servidores de la empresa en la ciudad de Lille -y, por su intermedio, de todos los dispositivos asociados a la Red- permitió a las autoridades monitorear (en muchos casos, en tiempo real) más de cien millones de mensajes encriptados[138], lo que a su vez derivó -tan solo en los Países Bajos- en el arresto de más de 100 personas, el secuestro de 8 toneladas de cocaína, 1.200 kilogramos de metanfetamina y casi € 20 millones en efectivo y el desmantelamiento de más de 19 laboratorios de drogas sintéticas[139], además de evitar la comisión de delitos gravísimos[140].

Lo que demuestra la operación concretada respecto de la red EncroChat (considerada como una de las mayores infiltraciones de una red criminal en la historia[141]) no es sólo el enorme valor del hackeo legal como herramienta de investigación contra la criminalidad organizada, sino también, en sentido opuesto, el *peligro que entraña dejarla de lado*. En efecto, la investigación de Europol deja perfectamente en claro que, en atención a la enorme capacidad de adaptación de los grupos criminales organizados y la amplia disponibilidad de herramientas tecnológicas aptas para sustituir a los medios tradicionales de comunicación, si el Estado renuncia al uso del *spyware*, está renunciando, en verdad, a su propia facultad de monitorear las comunicaciones de las organizaciones criminales más peligrosas y, por consiguiente, a perseguirlas eficazmente.

Semejante renuncia, por parte del Estado, importaría sustraerse (aun parcialmente) a su cometido esencial de asegurar la existencia pacífica de los ciudadanos, lo que según ROXIN equivale a desahuciarse así mismo, ya que el Estado moderno se justifica en tanto que garantiza a los ciudadanos la seguridad[142]. En esa dirección, cabe tener presente que el Estado no cumple con su tarea de seguridad solamente mediante la promulgación de leyes, sino mediante la *ejecución eficaz* de las mismas, por lo que cualquier tesitura que propicie la inaplicabilidad del Derecho penal está propiciando, en realidad, el abandono de la función que justifica la existencia del propio Estado[143].

Ahora bien: el reconocimiento de la legitimidad de llevar a cabo la interceptación de las comunicaciones mediante un *spyware* genera un interrogante adicional, derivado de la posibilidad de dotar a ese tipo de programas de funcionalidad múltiple (es decir, de convertirlos

---

intentos erróneos consecutivos de ingresar la contraseña o si el propio usuario teclea un PIN previamente establecido a tal efecto (ver: Europol (2020): "Dismantling of an encryted network…", cit.).

[138] Cfr. COX, Joseph (2020): "How police secretly took over a global pone network for organized crime", cit.

[139] Ver: Europol (2020): "Dismantling of an encryted network…", cit.

[140] Así, por ejemplo, como consecuencia de esta investigación las autoridades neerlandesas descubrieron que una de las organizaciones criminales desmanteladas había adquirido contenedores adaptados para fungir como cárceles y -en un caso- como cámara de torturas (ver: The Guardian: "Dutch arrests after discovery of 'torture chamber' in sea containers", publicado el 7/7/2020, obtenido en: https://www.theguardian.com/world/2020/jul/07/dutch-police-arrest-six-men-after-discovery-of-torture-chamber. También hubo arrestos en Francia, Inglaterra, Suecia y Noruega, en el marco de una investigación conjunta que ya reveló la existencia de más de un centenar de delitos y aportó información que para la apertura de cientos de investigaciones en toda Europa (al respecto, ver: NOSSITER, Adam (2020): "When police are hackers: Hundreds charged as encrypted network is broken", en *The New York Times*, publicado el 2/7/2020, obtenido en: https://www.nytimes.com/2020/07/02/world/europe/encrypted-network-arrests-europe.html).

[141] Cfr. COX, Joseph (2020): "How police secretly took over a global pone network for organized crime", cit.

[142] Cfr. ROXIN, Claus (1997), Derecho Penal. Parte General. Tomo I. Fundamentos. La estructura de la teoría del delito, Civitas, Madrid, págs. 64/65.

[143] Cfr. ISENSEE, Josef (2014), El derecho constitucional a la seguridad. Sobre los deberes de protección del Estado constitucional liberal, Rubinzal-Culzoni, Santa Fe, págs. 35 y ss. (énfasis en el original).

en "amenazas combinadas", capaces de ejecutar simultáneamente distintas modalidades de vigilancia). Puntualmente, si frente al uso de programas espías multifunción, el derecho al secreto de las comunicaciones otorga protección suficiente a los ciudadanos.

El problema aquí no radica en la coexistencia de distintas modalidades de telecomunicación, ya que no existe duda ni en la doctrina ni en la jurisprudencia en punto a que la protección constitucional otorgada por el referido derecho abarca todos los medios de comunicación conocidos en el momento de aprobarse la norma fundamental, así como los que han ido apareciendo o puedan aparecer en el futuro, no teniendo limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse[144]. Tampoco con la naturaleza del contenido de las comunicaciones, desde que, no obstante tratarse de un derecho claramente relacionado con el derecho fundamental a la "intimidad", el secreto de las comunicaciones no se identifica absolutamente con él, sino que posee un contenido mucho más amplio. En efecto, mediante el art. 18.3 de la CE el constituyente no ha querido proteger exclusivamente el secreto de las comunicaciones "íntimas", *sino cualquier clase de comunicación*, y ello con independencia de su contenido material, lo que ha llevado la doctrina española a proclamar el carácter "formal" de este derecho fundamental[145].

El problema real reside en que la infiltración clandestina de un sistema informático complejo ofrece la posibilidad de espiar el sistema en su totalidad, y no tan solo interceptar un intercambio aislado de comunicaciones como en las operaciones tradicionales de intervención telefónica[146]. En atención a ello, el BVerfG entendió, en el precedente en el que "creó" el derecho a la "integridad y confidencialidad de los sistemas de tecnología de las comunicaciones" que el art. 10.1 de la Constitución Alemana (similar al art. 18.3 de la CE) sólo brinda resguardo suficiente si la vigilancia se restringe únicamente a los datos emanados de una telecomunicación en curso. Si, en cambio, se utiliza la infiltración para recolectar datos distintos de los de las telecomunicaciones (por ejemplo, copiar información almacenada en el disco rígido), entonces la norma constitucional citada no resulta efectiva[147].

En este orden de ideas, se advierte que la propia regulación de la interceptación de comunicaciones incorporada por la LO 13/2015 se aparta del concepto de interceptación "pura" que podría amparar, por sí solo, el derecho consagrado en el art. 18.3 de la CE en favor de una concepción más amplia de la medida. En efecto, el art. 588 ter (b)(2) de la LEC dispone que la intervención judicialmente acordada puede autorizar el acceso no sólo al contenido de las comunicaciones y los "datos de tráfico", sino que también habilita expresamente la instrumentalización de la interceptación del equipo de comunicación para obtener datos no vinculados directamente a las comunicaciones del sospechoso. Lo expuesto queda en evidencia en el art. 588 ter (d)(2)(d), que prevé como uno de los objetivos de la medida "[e]*l conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación*".

[144] Ver, por todas, las SSTS 367/2001, de 22 de marzo y 1377/1999, de 8 de febrero.
[145] Cfr. GIMENO SENDRA, Vicente (2011): "La intervención de las comunicaciones telefónicas y electrónicas", en *Revista 39, Tribuna de Actualidad*, citado de documento electrónico obtenido en http://www.elnotario.es/index.php/hemeroteca/revista-39/697-la-intervencion-de-las-comunicaciones-telefonicas-y-electronicas-0-2863723191305737 (Con cita de las SSTC 114/1984 de 29 noviembre, 34/1996 de 11 marzo, 127/1996 de 9 julio, 58/1998 de 16 marzo, 123/2002 de 20 mayo, 70/2002 de 3 abril, 56/2003 de 24 marzo).
[146] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 113.
[147] Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 114.

Por añadidura, el ya mencionado art. 588 ter (d)(2), parágrafos (b) y (c) incluye, entre los objetivos posibles de la interceptación de la comunicación, poder determinar "[e]*l conocimiento de su origen o destino, en el momento en el que la comunicación se realiza*" y/o "[l]*a localización geográfica del origen o destino de la comunicación*". Esto es: los datos que se ven oscurecidos cuando cualquiera de los participantes en una comunicación utiliza una "herramienta de anonimato" como el sistema TOR, la red I2P o las redes privadas virtuales (VPNs), en la medida en que enmascaran las verdaderas direcciones IP desde las que dicho usuarios se conecta con la Internet.

Al respecto, cabe tener presente que sólo una pequeña parte del tráfico de Internet comprende a comunicaciones "entre humanos" como los *emails*. La mayoría de las comunicaciones en Internet son entre humanos y ordenadores, como las páginas en tránsito de la World Wide Web (WWW), los comandos enviados a servidores remotos y transferencias de archivos. Muchas otras involucran comunicaciones entre los propios ordenadores[148], como el tráfico administrativo de la Red que mantiene funcionando a la Internet. Dado que estas comunicaciones también pueden aportarle información al Estado[149], cabe preguntarse si son acaso estas disposiciones, en lugar de las referidas al acceso remoto a los sistemas informáticos, las que pueden dar amparo a la realización de "ataques de abrevadero" como los realizados por el FBI en los EE.UU. Es decir: aprovechar una comunicación para enviar un programa espía diseñado para introducirse en el "terminal o medio de comunicación" del usuario oculto tras una herramienta de anonimato y reportar su verdadera dirección IP o incluso su geolocalización.

Un obstáculo para admitir esta última interpretación podría residir en las exigencias previstas en el art. 588 ter (d)(1) de la LEC para la solicitud de orden judicial. Ello, desde que en el supuesto de que -por ejemplo- la investigación criminal este referida a los sujetos que, amparados por herramientas de anonimato, divulgan o descargan imágenes de explotación sexual infantil hacia o desde una página web ubicada en la "red oscura", los datos mencionados en los parágrafos (a) y (b) del citado art. 588 ter (d)(1) serán desconocidos, siendo que uno de los fines de la medida en estos casos es, precisamente, *obtener esos datos*, para luego recolectar la evidencia de cargo propiamente dicha mediante el registro físico o remoto del ordenador del usuario.

No obstante, podría entenderse que es posible "*identificar el medio de telecomunicación de que se trate*" consignando en la solicitud de orden judicial que la medida de interceptación de las comunicaciones se dirige -por ejemplo- contra los equipos de todos aquellos que se conecten con la página web antes mencionada y descarguen imágenes de explotación sexual infantil, explicando que el *spyware* se despliega infectando los contenidos ilícitos o el sistema de la página web de modo tal que, cada vez que alguien descarga su contenido introduce a su vez el

[148] El intercambio de datos entre ordenadores se produce cuando una de ellos, denominado "el cliente" ("*client*") le solicita información a otro (el "servidor" o "*server*"). Este proceso es facilitado por el Protocolo de Control de Transmisión ("*Transmission Control Protocol*" o TCP) y el Protocolo de Internet ("*Internet Protocol*" o IP), que combinados forman el TCP/IP (Cfr. HAMMEL SCHULTZ, David (2001): "Unrestricted federal agent: Carnivore and the need to revise the Pen Register Statute", en *Notre Dame Law Review*, Vol. 76, N° 4. pág. 122).

[149] Cfr. KERR, Orin S. (2003): "Internet surveillance law after the USA Patriot Act: The big brother that isn't", en *Northwestern University Law Review*, Vol. 97; N° 2, pág. 613.

programa espía en su dispositivo. Siendo así, ocurre que aunque en la solicitud -y luego en la eventual autorización judicial- no se identifique a un sospechoso en particular, ni tampoco un ordenador o equipo electrónico específico (individualizado mediante su número de abonado, de terminal o de etiqueta técnica), ni una dirección IP específica, si existirá certeza de que el programa espía ha sido enviado al terminal de un sujeto respecto del cual existen sospechas suficientes de que cometió un delito y de que en dicha terminal se encuentra evidencia del mismo. Ello, toda vez que el sospechoso sólo puede ser objeto de la medida si descarga las imágenes de explotación sexual infantil[150].

6. Vigilancia acústica y audiovisual

La reforma operada mediante la LO 13/2015 también incorporó en el art. 588 quater (a)(1) de la LEC la posibilidad de utilizar herramientas tecnológicas para obtener audio -y eventualmente imágenes de video- de "comunicaciones orales directas". Tal como está redactada, resulta indudable que la norma alude, principalmente, al uso de los denominados "dispositivos de espionaje sin cable" ("*wireless spy devices*" o WSDs), que son micrófonos o cámaras (con sonido) diseñados para ser colocados físicamente en objetos o prendas que uno de los interlocutores lleva encima; o escondidos en el espacio físico donde la conversación va a tener lugar, tales como salas de reuniones, oficinas o vehículos[151]. Al respecto, cabe señalar que si bien en los últimos años, el desarrollo de la tecnología en punto a la miniaturización de componentes electrónicos ha generado en forma simultánea un incremento de la capacidad de esta clase de dispositivos (tanto en términos de alcance como de calidad de la grabación) y una disminución de su tamaño, lo cual facilita su ocultación, lo cierto es que el principal riesgo operativo derivado de su uso sigue siendo la posibilidad de que sean descubiertos[152]. Ello, en la medida en que se trata de elementos que deben ser ubicados *físicamente* ya sea en la habitación o el vehículo en que se encuentra el sospechoso[153], o encima de una persona que se encuentra próxima a aquél (lo cual puede redundar, por ende, en la creación de un riesgo cierto para la integridad física de este último).

[150] A partir de la reforma introducida en el Código Penal Español a través de la LO 1/2015 de 30 de marzo, se amplió el catálogo de conductas típicas vinculadas a la pornografía infantil, castigando en el párrafo segundo del apartado quinto del art. 189 con la misma pena prevista para la posesión a quien acceda a sabiendas a pornografía infantil.

[151] Cfr. SATHYAMOORTHY, Dinesh / JALIS, Mohd / SHAFII, Shalini (2014): "Wireless spy devices: A review of technologies and detection methods", en *Defense, Science and Technology Technical Bulletin*, pág. 131. Estos dispositivos pueden ser activos o pasivos. Los primeros transmiten lo que graban (ya sea audio o video) en forma inalámbrica a través de radiofrecuencia a un receptor ubicado en las cercanías. Los dispositivos pasivos no transmiten señales, sino que únicamente graban lo que reciben en una memoria interna o en una tarjeta de memoria externa (Ibídem, pág. 132).

[152] Al respecto, cabe señalar que respecto de los dispositivos "activos" (es decir, los que transmiten lo que captan a otra locación en tiempo real), existen contramedidas que permiten su detección. Esto es: equipos detectores de radiofrecuencia (RF) que identifican las señales que emiten los dispositivos al acercarse a los mismos, los cuales se utilizan para realizar un "barrido" de las habitaciones o vehículos a efectos de localizar cualquier micrófono oculto (Cfr. SATHYAMOORTHY, Dinesh / JALIS, Mohd / SHAFII, Shalini: "Wireless spy devices…", cit., pág. 137). .

[153] Con relación a esta última circunstancia, el art. 588 quater (a)(2) de la LEC establece que "[e]n el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares".

Frente a ello, la posibilidad de recurrir al *spyware* en lugar de instalar un micrófono se erige como una alternativa viable, que permite sacar provecho de la circunstancia de que, en la actualidad, prácticamente todas las personas llevan consigo a todas partes sus teléfonos móviles y/o tienen ordenadores en sus viviendas y oficinas, los cuales pueden ser instrumentalizados para concretar la medida autorizada por el art. 588 quater (a)(1) *sin necesidad de acceder físicamente a los mismos*. En efecto, ha quedado demostrado que, en la práctica, tanto los teléfonos móviles como los ordenadores (o cualquier otro equipo similar, como una tableta) puede ser convertidos en un "dispositivo de espionaje sin cable" mediante un programa que toma el control del micrófono y las cámaras que esos equipos tienen instalados de fábrica, para grabar y transmitir en audio y video las conversaciones sostenidas en derredor del mismo.

Esta alternativa, conocida como de "micrófono errante" ("*roving bug*") o "micrófono caliente" ("*hot mic*") precede incluso a la aparición de los modernos teléfonos inteligentes. De hecho, las primeras menciones en la literatura especializada sobre la posibilidad de usar a los teléfonos móviles como micrófonos ocultos surgieron a comienzos del presente siglo[154], oportunidad en la que empezó a ser reconocida por los tribunales estadounidenses como una herramienta legítima de investigación criminal[155]. En la actualidad, los programas informáticos de espionaje avanzados en uso -como el "Smurf suite" de la Agencia de Seguridad Nacional (NSA) estadounidense o productos comerciales como "Pegasus"[156] o "FinFisher"- incluyen entre sus funciones la de encender remotamente el micrófono de los teléfonos móviles o las cámaras web de los ordenadores.

Al igual que con la interceptación de comunicaciones, el interrogante es si ante la ausencia de una mención expresa al uso de spyware como la contenida en el art. 588 septies (a) -que autorizaba la "instalación de un software"-, puede entenderse, o no, que el art. 588 quater (a) de la LEC legitima el recurso a este tipo de herramientas para llevar a cabo la captación de "comunicaciones orales directas".

---

[154] En los EEUU, el experto en seguridad informática Bruce SCHNEIER hizo referencia al tema por primera vez en 2006 (ver, al respecto: aut. cit.: "Remotely eavesdropping on cell phones microphones", publicado en "Schneier on Security" el 5/12/2006, documento informático obtenido en: http://www.bugsweeps.com/info/eavesdropping_detection.html). Sin embargo, ya en 2004, una nota publicada en la página web de la BBC mencionaba, entro otros métodos para escuchar conversaciones remotamente, la posibilidad de convertir a los teléfonos móviles en micrófonos ocultos, utilizando para ello las frecuencias que usan dichos aparatos para comunicarse con sus bases (distinta de la que se usa para hablar). Ver: BBC News: "This goes no further…", publicado el 2/3/2004, obtenido en: http://news.bbc.co.uk/2/hi/uk_news/magazine/3522137.stml.

[155] Ver: *United States v. Bianco*, 998 F.2d 1112, 1122-24 (Corte Federal de Apelaciones del 2° Circuito, 1993); *United States v. Gaytan*, 74 F.3d 545. 553 (Corte Federal de Apelaciones del 5° Circuito, 1996); *United States v. Petti*, 973 F.2d 1441 (Corte Federal de Apelaciones del 9° Circuito, 1992) y 507 U.S. 1035 (Suprema Corte de los EEUU, 1993).

[156] Éste último, aparentemente utilizado para vigilar ilegalmente a políticos en España en los últimos años. Al respecto, ver: La Vanguardia: "Pegasus: el móvil de Torrent fue espiado por un programa que solo se vende a gobiernos", publicado el 14/7/2020, obtenido en: https://www.lavanguardia.com/politica/20200714/482313919404/telefono-movil-roger-torrent-president-parlament-programa-espia.html; y El País: "El móvil del Presidente del Parlament fue objetivo de un programa espía que sólo pueden comprar los gobiernos", publicado el 13/7/2020, obtenido en: https://elpais.com/espana/2020-07-13/el-movil-del-presidente-del-parlament-fue-objetivo-de-un-programa-espia-que-solo-pueden-comprar-gobiernos.html.

Entiendo que así es. Y ello, por dos motivos. En primer lugar, porque la norma citada autoriza tanto la "colocación" como la "utilización" de "*…dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas*". Al respecto, me parece claro que, con esto, el legislador pretendió legitimar tanto la colocación de dispositivos electrónicos dirigidos a captar dichas comunicaciones, como a *utilizar dispositivos electrónicos que ya estaban en condiciones de captarlas* (sin necesidad de ser expresamente instalados por las autoridades a tal efecto). Por ejemplo, el teléfono móvil o el ordenador del sospechoso. De lo contrario, parecería redundante que la norma deba aclarar que *si se coloca un dispositivo de este tipo es para utilizarlo*. En segundo lugar, por cuanto, como ya se señaló respecto de la interceptación de las comunicaciones "no directas", no existe una afectación distinta de los derechos fundamentales en juego si se recurre a uno u otro método (dispositivo electrónico físico colocado por la autoridad estatal o instrumentalización de los equipos de la persona investigada). En los dos supuestos, de lo que se trata es de hacer cumplir la misma facultad legalmente asignada al Estado de restringir un derecho fundamental, sólo que de distintas maneras.

Esta pareciera ser también la interpretación de BUENO DE MATA, según el cual el citado art. 588 quater (a) apuesta por una tipología abierta, pensando en el devenir de la tecnología en los años futuros, al permitir a la Policía Judicial obtener y grabar por *cualquier medio técnico* imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos. Con todo ello, se amplía el catálogo de medios técnicos utilizados hasta el infinito con el único ánimo de que la legislación no caiga en una obsolescencia tecnológica con el paso del tiempo[157].

Cualquiera sea el método empleado para llevar a cabo la medida en análisis, es preciso establecer su alcance, en especial tomando en consideración el tenor de los derechos fundamentales afectados. Puntualmente, el derecho a la inviolabilidad del domicilio (art. 18.2 CE) y los derechos a la intimidad y al secreto de las comunicaciones (arts. 18.1 y 3 CE, respectivamente)[158]. En tal contexto, es el avance sobre el derecho a la intimidad lo que mayores reservas genera en orden al modo en que puede llegar a implementarse la medida de captación de comunicaciones orales directas. En orden a ello, VEGAS TORRES apunta que la posibilidad de que las escuchas se realicen incluso dentro del domicilio, y que pueda extenderse la grabación no solamente al sonido, sino también a la imagen, suponen una injerencia en el

[157] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.

[158] Al respecto, CASANOVA MARTÍ explica que existen dos grandes posiciones en la doctrina, en función del alcance que se dé del término "comunicación": a) por un lado, están los que entienden que el art. 18.3 CE protege todo tipo de comunicación independientemente del medio empleado, de manera que, obviamente también protege la comunicación directa realizada a través del aire; b) sin embargo, otros autores entienden que el art. 18.3 CE solo protege las comunicaciones que se realizan a través de algún medio técnico, quedando fuera de su alcance las simples conversaciones orales, por no ser comunicación en sentido estricto y dado que para ellas ya existe la protección del art. 18.1 CE. El autor se vuelca por la primera opción, señalando que, a su entender, las conversaciones directas entre dos o varias personas están dentro del alcance del art. 18.3 del texto constitucional, ya que se trata de una comunicación perfectamente protegible por el derecho al secreto de las comunicaciones (Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit.). En apoyo de su postura, el autor cita la STC 114/1984 del 29/11, en la que el tribunal manifestó que "*…sea cual sea el ámbito objetivo del concepto de comunicación, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros* […] *ajenos a la comunicación misma*".

ámbito de la intimidad de intensidad máxima[159]. En especial desde que, en un espacio privado bien puede ocurrir que dicha medida tenga efectos colaterales en personas que convivan con los sujetos investigados y que nada tengan que ver con el hecho delictivo que se trata de esclarecer, cercenando también la intimidad o la inviolabilidad del domicilio a aquellos que convivan con el investigado[160]. Por consiguiente, CASANOVA MARTÍ destaca que una medida que afecta tan directa y gravemente a la intimidad de las personas solo puede encontrar su justificación cuando lo que se persiga sea un delito grave, entendiendo que no solo ha de tenerse en cuenta la gravedad de la pena, sino también su trascendencia y repercusión social, como viene exigiendo la jurisprudencia del TS. Necesidad que se torna todavía más patente cuando la vigilancia acústica tiene lugar en el interior de un domicilio, puesto que constituyen una de las injerencias de mayor alcance y grado de afectación del derecho a la intimidad de las que el Estado puede ordenar[161].

Al respecto, el art. 588 quater (b)(2) establece que la vigilancia acústica o audiovisual solo puede autorizarse respecto de la investigación de ciertos delitos considerados graves y cuando pueda racionalmente preverse que por su intermedio se obtendrán datos esenciales y de relevancia probatoria. Sobre esta última disposición, CASANOVA MARTÍ apunta que poco habría que decir si la literalidad de este artículo realmente se ciñera a delitos de especial gravedad, pero no es el caso. En esa dirección, explica que, si bien es correcto que el legislador ha legitimado la práctica de esta medida en la investigación de delitos cometidos en el seno de organizaciones criminales y terrorismo, el límite impuesto en el inciso (b)(2)(a) no permite reservar exclusivamente una medida tan intrusiva solo a los delitos más graves del Código Penal[162].

En orden a ello, resulta de sumo interés la postura adoptada por el BVerfG sobre la cuestión, mucho más rigurosa en términos de protección de la intimidad frente a la vigilancia acústica que la elegida por el legislador español en la LO 13/2015. En efecto, en un fallo dictado en 2004[163], referido a la constitucionalidad de una normativa procesal que autorizaba la vigilancia acústica de los hogares, el referido tribunal enfatizó el vínculo entre la inviolabilidad del domicilio, la dignidad humana y el mandamiento jurídico constitucional de respetar necesariamente una esfera del ciudadano dentro de la cual éste pueda desarrollarse de manera personalísima[164]. En tal contexto, señaló que existe un núcleo inviolable, en el que el particular desarrolla su vida privada, que debe ser respetado por el Estado al llevar a cabo medidas de vigilancia[165], de modo tal que cualquier injerencia estatal dentro de dicho núcleo lesiona la libertad conferida a cada persona para desarrollarse libremente, especialmente tratándose de asuntos personalísimos.

Cabe aclarar, en este punto, que el BVerfG no estableció que la vigilancia acústica del domicilio particular con el objetivo de perseguir los delitos lesione *en forma general* el contenido de

[159] Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", cit., pág. 5.
[160] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.
[161] Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit. Con cita de SSTS 938/2013 (del 10/12) y 503/2013 (del 19/6).
[162] Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit. Con cita de SSTS 938/2013 (del 10/12) y 503/2013 (del 19/6).
[163] Sentencia BVerfG 109, 279 (rta. 30/3/2004).
[164] Fallo citado. Con cita, a su vez, de BVerfG 75, 318 y BVerfG 51, 97.
[165] Con relación a esta garantía, citó los precedentes BVerfG 6, 32; 27, 1; 32, 373; 34, 238; y 80, 367.

protección de la dignidad humana, sino que es *la forma y modo* en que se lleva a cabo la vigilancia del domicilio particular lo que puede conducir a una situación en la que se ocasione dicha lesión. Con relación a ello, el tribunal explicó que la vigilancia acústica del domicilio particular atenta contra la dignidad humana cuando no se respeta el ámbito dentro del cual se desarrolla la vida privada[166]. Para determinar si una conducta debe ser ubicada dentro de este ámbito absolutamente protegido, debe considerarse si su contenido es de carácter personalísimo, así como la manera y la intensidad en la que dicha conducta incide en la esfera de otros o en los asuntos de la comunidad, para lo cual resultan determinantes las particularidades del caso concreto.

En dicho orden de ideas, el Tribunal Constitucional fue terminante en señalar que ni siquiera los intereses preponderantes de la colectividad pueden justificar una injerencia en ese ámbito de la personalidad absolutamente protegido[167]. Así, concluyó afirmando que la vigilancia acústica del domicilio particular con el fin de perseguir los delitos no puede penetrar este ámbito de protección *en ningún caso*, ni siquiera en aras de la efectividad de la administración de justicia o con el objeto de investigar la verdad de los hechos[168]. Y ello, a pesar de reconocer que pueden existir casos especialmente graves de criminalidad, con las correspondientes situaciones de sospecha, en los cuales la efectividad de la administración de justicia penal pudiera llegar a parecer más importante que la protección de la dignidad humana del inculpado; no obstante lo cual reiteró que, incluso en esos casos, al Estado *le está prohibido realizar una valoración de este tipo* conforme el principio de proporcionalidad.

Sin perjuicio de ello, el BVerfG explicó que, aunque el domicilio particular constituye un "último refugio" para la dignidad humana, ello no exige *una protección absoluta de todos los espacios de la vivienda particular*, sino que sólo corresponde respetar en forma absoluta la conducta desarrollada en dichos espacios, en la medida en que tal conducta se vincule con "el desarrollo de la propia existencia". Por ende, a las autoridades les está prohibido escuchar las conversaciones privadas que una persona sostiene en el interior de su domicilio particular, cuando la persona se encuentre sola o exclusivamente en compañía de personas respecto de las cuales tiene una relación de particular confianza –pertenecientes al núcleo absolutamente protegido–, como pueden ser los familiares y los conocidos más allegados, y cuando no existan indicios concretos de que las conversaciones que están por realizarse –atendiendo a su contenido– tengan un nexo o relación directa con la realización de un delito[169].

---

[166] Al respecto, el BVerfG explicó que el desarrollo de la personalidad en el núcleo de la configuración de la vida privada abarca la posibilidad de manifestarse libremente en los procesos internos –tales como sensaciones y sentimientos, así como pensamientos, puntos de vista y vivencias de carácter personalísimo– y ello sin miedo a la vigilancia por parte de los órganos estatales. De la protección abarca también la manifestación de sentimientos, manifestación de las experiencias del subconsciente, así como formas de expresión de la sexualidad.

[167] Con cita de BVerfG 34, 238.

[168] La protección de este espacio de intimidad también había sido puesta de resalto por el BVerfG en el fallo en el que creó el derecho a la "confidencialidad e integridad de los sistemas de tecnología de la información" (analizado *Supra*, § 4), oportunidad en la que destacó que cualquier medida que restringiese dicho derecho debía garantizar que no se violentase el núcleo de la conducción de la vida privada, por considerarlo un derecho absolutamente fundamental que no puede ser restringido de ningún modo (Cfr. ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court…", cit., pág. 121).

[169] El BVerfG explica que si bien las conversaciones que cada quien sostiene en su domicilio particular con sus personas más allegadas no pertenecen de suyo al ámbito del desarrollo de la vida privada, existe una presunción en este sentido. Señaló también que para evitar que la vigilancia acústica se entrometa en áreas constitucionalmente protegidas, la autoridad debe asegurarse –mediante investigaciones previas

Por tanto, una vigilancia de carácter *general* –en lo que se refiere al tiempo y al espacio-, en principio, no puede permitirse, porque la probabilidad de abarcar conversaciones de carácter personalísimo es muy alta[170]. Sin embargo, conforme las premisas establecidas por el BVerfG si puede admitirse una vigilancia acotada temporalmente, respecto –por ejemplo- de una reunión sostenida dentro de la vivienda del sospechoso y entre éste y una persona que no pertenezca al núcleo absolutamente protegido (así, por ejemplo, un cliente o un socio de negocios, o una persona sospechadas de ser cómplice del dueño de casa en una empresa o actividad criminal), cuando concurran motivos previos suficientes para sospechar que pueden discutirse asuntos relativos a las conductas ilícitas objeto de investigación

Vinculado a lo expresado en el fallo mencionado *Supra*, es menester tener presente que el legislador español previó, en el art. 588 quater (b)(1) que "[l]*a utilización de los dispositivos a que se refiere el artículo anterior ha de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación*"[171]; como así también que la eventual resolución judicial que autorice la medida debe contener tanto la identificación del lugar en que va a llevarse a cabo como del encuentro del investigado que se pretende vigilar[172].

En opinión de CASANOVA MARTÍ, el hecho de que las normas citadas no contengan referencia alguna a la duración de la medida constituye un grave descuido del legislador. El autor argumenta, en tal sentido, que la colocación de aparatos de escucha y transmisión del sonido con carácter permanente o indefinido supondría convertir esta medida en las propias de un Estado policial, lo cual provocaría un abuso al sistema democrático. Por lo tanto, considera que es necesario que el legislador establezca un plazo de duración máximo durante el cual pueda mantenerse legítimamente la intervención, así como especificar los momentos de inicio y finalización del cómputo[173].

En sentido opuesto, tengo para mí que la forma en que ha sido regulada la aplicación de esta medida de vigilancia acústica o audiovisual es más eficaz para evitar la vulneración de los derechos fundamentales en juego que la alternativa de duración en términos temporales fijos que propicia CASANOVA MARTÍ. En efecto, lo que se autoriza conforme lo dispuesto en el 588 quater (b)(1) de la LEC no es una vigilancia más o menos prolongada de lo que se habla en una vivienda u otra locación, sino que se ha previsto una medida mucho más específica, dirigida a capturar *una conversación en particular que se anticipa va a tener lugar*. Por ende, si la vigilancia excede el lapso temporal en el que se sospecha que puede verificarse *esa conversación* específica, deja de ser legítima en los términos de la norma. En contraposición, una regulación

---

que dejen a salvo la protección del ámbito de desarrollo de la vida privada– que la vigilancia acústica del domicilio particular quede limitada exclusivamente a procesos y hechos que sean relevantes desde el punto de vista procesal.

[170] En dicha línea, el BVerfG recomendó también que las autoridades al vigilar un domicilio particular prescindan de la utilización de mecanismos automáticos de grabación, de modo que puedan interrumpir la grabación en cualquier momento. De ese modo, si en el marco de una medida de vigilancia acústica llega a presentarse una situación que deba ser atribuida al ámbito inviolable de desarrollo de la vida privada, la medida de vigilancia puede ser interrumpida inmediatamente. Las grabaciones que, no obstante, se hubieren obtenido, deberán ser destruidas.

[171] Énfasis añadido.

[172] Art. 588 quater (c) de la LEC.

[173] Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit.

que autorice la vigilancia de esta clase por un tiempo prefijado, aunque sea breve (varias horas, por ejemplo) parece mucho menos eficaz para evitar que durante ese lapso temporal se produzca una injerencia sobre el núcleo de la vida privada, del tipo de las que prohíbe el fallo del BVerfG.

De igual manera, cabe señalar que desde el punto de vista práctico, el modo en que ha sido regulada la implementación de esta medida también torna aconsejable el recurso a un *spyware*, toda vez que éste puede dejarse instalado (pero inactivo) en el teléfono móvil o el ordenador (o en las cámaras web de vigilancia activables por Internet) del sospechoso y *activarse sólo en el momento en que se supone que está por ocurrir la conversación relevante y por el término de la duración de la misma*. De este modo, se evitan los problemas logísticos y riesgos derivados de tener que colocar un dispositivo físicamente en cada ocasión en la que se prevea que puede producirse una conversación de interés para la investigación.

7. Seguimiento y localización. Operaciones encubiertas

En el contexto tecnológico actual conviven dos realidades antagónicas en relación con la posibilidad estatal de establecer en dónde se encuentra un sospechoso (o un simple ciudadano) en un momento dado, o cuando lleva a cabo una determinada acción. Por un lado, los avances tecnológicos -en especial la aparición de los sistemas GPS y su uso generalizado en vehículos y en los propios teléfonos móviles, que casi todos los ciudadanos llevan consigo a todas partes- han derivado en que el seguimiento continuo, prolongado y en tiempo real de un sospechoso, que hace una década era una medida excepcional y reservada a los casos más relevantes (debido a su elevado costo en términos de recursos humanos, materiales y presupuestarios), hoy pueda llevarse a cabo de forma casi rutinaria y generalizada. Por el otro, el surgimiento de las herramientas informáticas "de anonimato" permite a las personas concretar toda clase de actividades (lícitas o ilícitas) a través de la Internet manteniendo en reserva su identidad y su ubicación, mediante el simple recurso de enmascarar la dirección IP desde la que se ingresan a la red.

En lo tocante a la primera cuestión, el art. 588 quinquies (b)(1) de la LEC ahora permite al juez competente "*...autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización*"[174]. A los efectos del presente trabajo, centrado en analizar qué grado de sustento normativo tiene el uso de *spyware* como medio de investigación en España, cabe señalar que la circunstancia de que el legislador haya optado por aludir tanto a "dispositivos" como "medios técnicos" entre las modalidades posibles para el cumplimiento de la medida de seguimiento permite concluir -aunque no se mencione en forma expresa el recurso a un programa informático- que no sólo se habilita el rastreo de un sospechoso colocando físicamente un dispositivo de seguimiento en su persona o su vehículo, sino también la posibilidad de concretarlo encendiendo remotamente el GPS que ya viene instalado en los teléfonos móviles a través de la instalación de un *spyware*. Esto es: recurriendo al hackeo legal del *smartphone*[175].

[174] Énfasis añadido.

[175] Una tercera alternativa radica en efectuar el seguimiento en tiempo real instrumentalizando la permanente comunicación que existe entre los teléfonos móviles y las antenas de telefonía celular, que permiten llevar a cabo dicho rastreo con la colaboración de la empresa de telefonía celular. A ello responde lo establecido en el art. 588 quinquies (b)(3) en cuanto dispone que "[l]*os prestadores, agentes y personas a que se refiere el artículo 588 ter e están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas*

En este sentido, entiendo que es válido para la medida de seguimiento y localización lo señalado en los apartados anteriores en orden a otras medidas de investigación incorporadas por la LO 13/2015, puntualmente que la interpretación según la cual dichas disposiciones legitiman también su concreción a través de programas informáticos "espías" no es menos garantista que la postura contraria, dado que no se traduce en una mayor injerencia sobre los derechos fundamentales de los ciudadanos, sino que se trata únicamente de producir *la misma injerencia por otros medios*.

La acertada decisión del legislador español de exigir autorización judicial expresa para la implementación de esta medida[176] evitó que se cayera en la discusión -que si se dio en otras latitudes- sobre si se requiere, o no, dicha autorización judicial cuando los seguimientos se restringen a los movimientos del imputado en calles públicas o cuando se prolongan en el tiempo, permitiendo de este modo que se conforme un "mosaico" que revela información protegida por el derecho a la intimidad del imputado[177]. En esa dirección, también resulta un acierto que el propio art. 588 quinquies (b) (1) exija, para justificar la autorización judicial, la concurrencia de "*…acreditadas razones de necesidad*" y la demostración de que la medida resulta proporcionada.

En esa dirección, igualmente positivo es que se haya fijado un límite máximo de tres meses a la duración de la medida en el art. 588 quinquies (c)(1) de la LEC. Sin embargo, la posibilidad prevista en la norma de prorrogarla hasta dieciocho meses parece excesiva, incluso teniendo en cuenta que el propio texto legal la define como "excepcional". Ello, desde que un seguimiento tan prolongado, teniendo en cuenta el grado de precisión que ofrecen los modernos dispositivos GPS y -en especial- la posibilidad de combinar la información que surja de la medida con otros datos de libre acceso para los investigadores, permite construir una suerte de "mosaico" con datos aparentemente inocuos que termina siendo tremendamente intrusivo en la intimidad del sujeto pasivo de la vigilancia.

Al respecto, la ministra Sotomayor de la Suprema Corte de los EE.UU. fue muy elocuente al expresarse sobre la cuestión en su voto concurrente en el precedente *United States v. Jones*[178], oportunidad en la que explicó que el monitoreo a través de GPS genera un registro preciso y

---

para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia".

[176] Ello, sin perjuicio de que el art. 588 quinquies (b)(4) admita que "[c]uando concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial [pueda] proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso".

[177] Estas cuestiones se discutieron, en los EE.UU., en los famosos precedentes *United States v. Knotts* (460 U.S. 276; 1983) y *United States v. Karo* (468 U.S. 705; 1984), en los que se analizó la legitimidad, bajo la protección a la "expectativa razonable de privacidad" de los ciudadanos consagrada en la 4ª Enmienda de la Constitución de ese país, del seguimiento efectuado con la asistencia de "beepers" exclusivamente en calles públicas o incluyendo también el ingreso de los dispositivos en la vivienda de los sospechosos. Posteriormente, la cuestión del seguimiento en calles públicas, pero prolongado por casi un mes, fue sopesada nuevamente por la Suprema Corte estadounidense en el precedente *United States v. Jones* (565 U.S. 400; 2012).

[178] 565 U.S. 400 (2012).

exhaustivo de los movimientos públicos de una persona, que revela un cúmulo de detalles sobre sus vínculos sociales, políticos, profesionales, religiosos y sexuales. Ello, toda vez que en el transcurso de una vigilancia extensa el sospechoso de seguro hará viajes cuya naturaleza indiscutiblemente privada no es difícil de imaginar: a un psiquiatra, un cirujano plástico, una clínica de abortos, un centro de tratamiento para el HIV, un club de desnudistas, un abogado penalista, un hotel por horas, una asamblea sindical, la mezquita, sinagoga o iglesia, el bar gay y muchas otras posibilidades. Registros que el Estado puede almacenar para minarlos efectivamente en busca de información durante muchos años en el futuro[179].

Por otra parte, en lo tocante a la "localización" de un sospechoso que este interactuando a través de Internet y cuya ubicación geográfica real no pueda establecerse debido a que actúa bajo el amparo de una herramienta informática de anonimato que enmascara su (verdadera) dirección IP, el método más novedoso combina la medida de acceso remoto a un sistema informático prevista en el art. 588 septies (a), analizado en el apartado § 5, con la figura del "agente encubierto digital" incorporado en el art. 282 bis (6) de la LEC por la LO 13/2015.

Se trata ésta última de una figura que venía siendo utilizada desde hace tiempo en España, y que necesitaba de una reforma y actualización urgente, para otorgarle la cobertura legal urgente que necesitaban y acabar con los vacíos legales que sobrevolaban sus actuaciones[180]. Sobre el punto, cabe tener presente que el agente encubierto informático viene a ser una especie dentro de la figura genérica de agente encubierta actualmente prevista en el art. 282 bis (1) de la LEC. En tal contexto, y en lo que respecta específicamente a la actuación en el "ciberespacio", el parágrafo (6) legitima al juez de instrucción a "…*autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a*". Esto es: amplía el catálogo de delitos investigables mediante el uso de un agente encubierto (en este caso, informático) para incluir también a los "…*cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*"[181].

Por añadidura, el segundo párrafo del art. 282 bis (6) dispone que "[e]*l agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*". La última parte de esta disposición es criticada por RUBIO ALAMILLO, quien explica que habida cuenta que el término "algoritmo" alude, en informática, a un procedimiento que resuelve un problema, no se entiende muy bien qué quiere expresar el legislador cuando indica que ha de ejecutarse un procedimiento informático para identificar un archivo ilícito que el propio agente informático ha enviado a un potencial delincuente, toda vez que dicho archivo señuelo ya debería estar totalmente identificado,

[179] Ver voto concurrente de la *Justice* Sotomayor en *United States v. Jones* (565 U.S. 400; 2012), pág. 3.
[180] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.
[181] Sin perjuicio de lo cual, BUENO DE MATA entiende que sería conveniente ampliar el listado de causas por las que un agente puede intervenir, incluyendo los delitos cometidos a través de la Red relacionados con víctimas especialmente vulnerables, para que los mismos pudieran actuar en operaciones contra la pederastia y el intercambio de material pornográfico o el ciberterrorismo, y al mismo tiempo contra delitos que se dan a través de redes sociales como como el *grooming*, el *ciberbulling*, el *stalking* o la e-violencia de género (Cfr. aut. cit., (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit).

indexado junto a otros ficheros utilizados para el mismo fin en una base de datos policial centralizada[182]. Lo que esta crítica omite valorar, empero, es que la norma no sólo alude al "envío" de archivos ilícitos sino a su "intercambio", por lo que -según entiendo- la mención al análisis de los algoritmos refiere a los archivos que el agente informático reciba *como resultado del intercambio*, provenientes del sospechoso.

En tal contexto, la evaluación a la que alude el art. 282 bis (6), 2° párrafo habrá de dirigirse a los "metadatos" de los archivos[183], en busca de información como -por ejemplo- el equipo en el que fueron creadas imágenes de explotación sexual infantil, o datos de geolocalización, etc. Sin embargo, no es ese el único modo de obtener, a través del intercambio permitido por la norma, información relevante sobre la identidad o la localización de un sospechoso. Por el contrario, al amparo de la disposición en trato y de la prevista en el art. 588 septies (a)(1), también puede autorizarse el envío, por parte del agente encubierto informático, de archivos que contengan un programa espía, a los efectos de que éste se introduzca en el ordenador del sospechoso y "reporte" a su base los datos que permitan obtener una ubicación geográfica precisa del mismo, así como establecer su verdadera identidad.

Como ya adelanté, esta mecánica viene siendo utilizada ya en otras jurisdicciones -en especial en los EE.UU.- y no sólo con respecto a sospechosos específicos e individuales, sino de modo general contra todos los visitantes de páginas web dedicadas a la actividad ilícita, en el marco de grandes operaciones encubiertas como las que suelen llevarse a cabo en los países de tradición legal anglosajona. La más notoria de estas operaciones es la que tuvo lugar en el denominado caso "Playpen" (también llamada "Operación pacifier"), que se inició en 2014 cuando el FBI fue alertado sobre la existencia de una página web dedicada a la distribución de imágenes de explotación sexual infantil, que se creía estaba basada en los EE.UU. A partir de ese dato, la agencia logró localizar el servidor que alojaba la página en el Estado de Florida, pero ante la imposibilidad de identificar a los clientes de la misma debido a que accedían a través del sistema TOR, el FBI optó por tomar el control de los servidores de Playpen y, tras obtener autorización judicial a tal efecto, infectó la página con un *spyware* que se introdujo en los ordenadores de todos los usuarios que descargaron imágenes de explotación sexual infantil durante el período en que estuvo activo. Una vez dentro, este *software* envió subrepticiamente a la sede del FBI la verdadera IP y otros datos identificatorios de los ordenadores de los usuarios. De ese modo, la agencia pudo establecer la ubicación geográfica de los sospechosos y requerir órdenes de allanamiento respecto de sus equipos en cada una de las jurisdicciones en las que se encontraban[184].

---

[182] Cfr. RUBIO ALAMILLO, Javier (2015): "La informática en la reforma…", cit.

[183] Los "metadatos" no son información creada por el usuario ("datos activos" o "active data") sino información *sobre la información*: fecha de creación de los documentos, autor, cambios efectuados, datos sobre el sistema o equipo con el que fueron creados, datos de transmisión, etc.; a la que por lo general se puede acceder solo operando digitalmente (esto es: no aparecen por defecto en las pantallas). Por ejemplo, el tristemente célebre asesino en serie Dennis Rader (conocido como "BTK", por las siglas en inglés de "atar-torturar-matar"), fue finalmente atrapado en 2005 cuando envió a las autoridades un disco de computadora conteniendo imágenes de una escena del crimen que no le había sido atribuido sacadas por él mismo. Los metadatos en un archivo de Word almacenado en el mismo disco indicaban que había sido creado en una iglesia luterana de Kansas y que el último en modificarlo había sido "Dennis". A partir de ello, la policía logró identificar a Rader como el presidente del consejo de dicha iglesia. Un registro posterior en el automóvil de Rader encontró evidencia de ADN de una de sus víctimas, lo que derivó en el arresto del nombrado y su posterior confesión.

[184] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., págs. 13/14.

Si se trata de trasladar al contexto español la posibilidad de llevar adelante este tipo de operaciones -que encuadran en la metodología conocida como "ataque de abrevadero", descripta *Supra* en el apartado § 2- entiendo que la principal dificultad no reside tanto en el aspecto vinculado a la infiltración de los ordenadores de los usuarios mediante el uso de un programa espía -en tanto encuentra sustento normativo expreso en el ya mencionado art. 588 septies (a)(1) de la LEC-, sino en establecer si el art. 282 bis del mismo cuerpo legal ampara una actividad encubierta estatal de esas características.

Al respecto, cabe tener presente, en primer lugar, que en cuanto atañe específicamente a la infiltración de foros de explotación sexual infantil como lo era la página "Playpen", el hecho de que funcionen al amparo de los "servicios ocultos" que ofrece el sistema TOR determina que constituyan espacios online cerrados y protegidos, difíciles de identificar y localizar y en cuyo seno los miembros son cuidadosamente seleccionados para evitar la posibilidad de infiltración[185]. En este marco, es habitual que estas comunidades demanden, como medida de seguridad, el intercambio de imágenes ilícitas en forma regular tanto a sus miembros como a los propios sitios web. Ello importa que para que la infiltración pueda ser efectiva, es forzoso que el agente encubierto digital -ya sea que tome el lugar de un "cliente" o, como en el caso "Playpen", suplante al administrador de la página- comparta también imágenes de explotación sexual infantil.

En ese orden de ideas, ya de por sí resulta polémica en España la facultad de compartir archivos ilícitos que el legislador le ha asignado al agente encubierto informático, rechazada por una parte de la doctrina que destaca, por un lado, que no puede existir un engaño a cualquier precio y se deben tener siempre presentes los principios de necesidad y proporcionalidad[186]; y por el otro que supone una incitación a cometer una actividad delictiva el envío de un fichero ilícito a un ciudadano, tanto más cuando el delincuente real puede diseminar estos archivos por la Red sin control, siendo encontrados en intervenciones domiciliarias por la Policía Judicial y sin saber si realmente dichos ficheros fueron enviados por la Policía como *señuelo*[187].

Entiendo que las objeciones antes citadas han sido debidamente atendidas por el legislador español en el art. 282 bis, en cuanto dispone por un lado la obligación del agente encubierto de "*…solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables"* cuando su actuación pueda afectar derechos fundamentales[188]; como así también que la actuación de éste último sólo está exenta de responsabilidad criminal en la medida en que "*…guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito"*[189]. En cuanto a la posibilidad de una difusión descontrolada de los archivos enviados por el agente encubierto, cabe señalar que los riesgos que ellos entraña pueden reducirse considerablemente mediante el simple recurso de identificarlos como tales mediante un código hash específico que se mantenga debidamente registrado y archivado. En cuanto a las objeciones éticas vinculadas a criterios filosóficos o de política criminal contrarios al uso del agente encubierto, la respuesta excedería el espacio disponible en este trabajo, pero basta señalar que, a mi modo de ver, no

[185] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., pág. 9.
[186] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.
[187] Cfr. RUBIO ALAMILLO, Javier (2015): "La informática en la reforma…", cit (énfasis añadido).
[188] Art. 282 bis (3).
[189] Art. 282 bis (5).

son congruentes con la realidad que actualmente enfrenta la persecución de ciertos delitos -muy especialmente, la explotación sexual infantil-, que se tornaría virtualmente imposible sin contar con estas herramientas legales.

Mucho más concreto y difícil de resolver es el dilema ético que representa la posibilidad de que el agente encubierto digital comparta, a los efectos de ser eficaz en su labor de infiltración, imágenes de explotación sexual infantil de *víctimas reales*, toda vez que no sería irrazonable concluir que el solo hecho de que el agente encubierto comparta material de esa clase –aun cuando, por supuesto, no haya sido generado por él- implicaría siempre una renovada victimización de los menores que aparecen en aquellas. Situación que se acentúa todavía más cuando se trata de operaciones de la envergadura de la concretada en el caso "Playpen", que involucran el intercambio de centenares o miles de imágenes.

Así, en la ya mencionada "Operación pacifier", el FBI no sólo operó la página web desde sus propios servidores durante casi dos semanas[190], sino que incluso mejoró la performance del sitio web para atraer más clientes, incrementando la membrecía en un 30% y cuadruplicando la cantidad de visitantes durante ese lapso[191]. En atención a dicha circunstancia, algunas defensas alegaron que el accionar del FBI fue tan "escandaloso" ("*outrageous*") que ameritaba la desestimación de los cargos. Señalaron, en tal sentido, que durante los 13 días en los que dicha agencia operó la página, se intercambiaron al menos 48.000 imágenes, 200 videos y 13.000 links a otros sitios de explotación sexual infantil. Sin embargo, los tribunales de apelación rechazaron estos argumentos, ponderando como contrapeso el peligro que entrañaba la disponibilidad de material de explotación sexual infantil en la Red. En esa dirección, destacaron que a sólo un año de su lanzamiento la página Playpen había alcanzado los 215.000 miembros y recibía más de 10.000 visitas semanales. Concluyeron, en consecuencia, que frente a la difícil disyuntiva a la que se enfrentaba el Estado, la mejor forma de aprehender a la mayor cantidad posible de criminales y proteger más eficazmente a las víctimas era manejar el servidor por un tiempo limitado[192].

En el marco de la discusión doctrinaria en España, BUENO DE MATA rechaza la posibilidad de intercambiar material delictivo obtenido en antiguas redadas, por considerar que de ese modo se sigue cometiendo el hecho punible por los agentes y se menoscaban los derechos de las víctimas. En sentido opuesto, el autor se decanta por permitir intercambiar "material camuflado creado *ad hoc*", es decir material pornográfico en el que aparezcan actores y actrices porno mayores de edad haciéndose pasar por menores de edad[193]. Si bien esta última posibilidad no parece factible en atención a la naturaleza del material que, en la realidad, es intercambiado en los foros de explotación sexual infantil (muy difícil de reproducir en forma verosímil por actores adultos)[194], entiendo que los últimos desarrollos tecnológicos en materia

[190] Cfr. AUCOIN, Kaleigh E.: "The spider's parlour…", cit., pág. 1449 (citas omitidas).
[191] Cfr. NUÑEZ, Michael (2017): "FBI drops all charges in child porn case to keep sketchy spying methods secret", en *Gizmodo*, publicado el 7/3/2017, obtenido en: https://www.gizmodo.com.au/2017/03/fbi-drops-all-charges-in-child-porn-case-to-keep-sketchy-spying-methods-secret/.
[192] Cfr. AUCOIN, Kaleigh E. (2018): "The spider's parlour…", cit., págs. 1451/1452 (citas omitidas).
[193] Cfr. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015…", cit.
[194] Ello, dado que en los foros donde se desarrolla la actividad cuya persecución reviste mayor prioridad para las autoridades se intercambian imágenes de explotación sexual de niños muy menores, imposibles de reproducir por medio de actores adultos.

de video (en especial la aparición de los denominados "*Deep fakes*"[195]) ofrecen una solución para generar, a partir de la manipulación de los archivos reales secuestrados por las autoridades, material apócrifo realista pero sin vinculo concreto con víctimas verdaderas, apto para ser utilizado por los agentes encubiertos informáticos en el cumplimiento de sus funciones.

8. Requisitos generales

La necesidad de fijar de modo preciso los límites al alcance de las distintas variantes de uso de *spyware* habilitadas mediante la reforma operada por la LO 13/2015 se desprende claramente de lo dispuesto por en el art. 18.4 de la CE. A tal efecto, se han incorporado en el art. 588 bis de la LEC una serie de "principios rectores" comunes para todas estas medidas de investigación tecnológica, estableciendo que deben satisfacer los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad[196], cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados[197].

El legislador español enumeró expresamente, en el art. 588 bis (a)(4) y (5) de la LEC, los elementos que el juez ha de tomar en consideración a la hora de ponderar los intereses en juego, y por tanto, a la hora de decidir acerca de la proporcionalidad de una medida de investigación telemática[198]. Así, en el primero de los parágrafos mencionados, se dispone que "[e]*n aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida: a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida*". Al respecto, se aprecia que la opción b) parece ser más flexible que la a), desde que en el primer supuesto supone que la medida restrictiva sea "indispensable" (por no existir ninguna otra medida menos gravosa que pueda ser útil para esclarecer el hecho); mientras que en el segundo sólo se exige que la obtención de la información buscada se vea "gravemente dificultada" en caso de no recurrirse a la misma.

Por añadidura, en el art. 588 bis (a)(5) de la LEC se prevé, en primer término, un criterio general para la evaluación de la proporcionalidad, enumerándose a continuación los parámetros que debe ponderar el juez como contrapeso a la intensidad de la injerencia sobre los derechos fundamentales. Sobre el punto, se señala que el criterio general de ponderación elegido por el

[195] Se denomina "*Deep fakes*" a videos alterados digitalmente mediante el uso de "redes (neuronales) generativas adversariales" (GANs, por sus siglas en inglés), que son sistemas de inteligencia artificial que producen videos nuevos a partir de la comparación y categorización de imágenes anteriores. Al respecto, ver: CHESNEY, Bobby / CITRON, Danielle (2019): "Deep fakes: A looming challenge for privacy, democracy, and national security", en California Law Review, Vol. 107 (citado de documento informático obtenido en: https://scholarship.law.bu.edu/faculty_scholarship/640/); y SCHWARTZ, Oscar (2018): "You thought fake news were bad? Deep fakes are were the truth goes to die", en The Guardian, publicado el 12/11/2018, obtenido en: https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth.

[196] Art. 588 bis (a)(1).

[197] Cfr. LÓPEZ-BARAJAS PEREA, Inmaculada (2017): "Nuevas tecnologías aplicadas…", cit., pág. 66.

[198] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 16.

legislador ya estaba consolidado tanto en la doctrina como en la jurisprudencia[199] con anterioridad a la reforma introducida mediante la LO 13/2015. Lo novedoso es que se haya señalado expresamente cuáles son los elementos relevantes para valorar el interés público[200].

La LEC también regula con bastante precisión, en su artículo 588 bis (c), los requisitos que debe reunir la resolución judicial que autorice la aplicación de una de estas medidas de investigación tecnológica, que vienen a sumarse a la regla básica demandando que la autorización se emita mediante auto motivado y previa opinión del Ministerio Fiscal. De este modo, conforme la concepción del legislador de 2015, lo que se pretende es que sea el propio juez, ponderando la gravedad del hecho que está siendo objeto de investigación, el que determine el alcance de la injerencia del Estado en las comunicaciones particulares[201]. En esa dirección, se le confiere al magistrado instructor el control no solo de la procedencia de la medida, por su necesidad y proporcionalidad, sino también del modo en que se ejecutará la misma, indicando la duración y los plazos para someter los resultados a su control (dentro de los límites fijados en la LEC para cada una de las medidas), así como el tipo de *software* que se instalará en el terminal a registrar, el modo en que serán aprehendidos los datos y también si los agentes pueden realizar copias de esos datos y, en tal caso, cómo habrán de conservarse para garantizar su autenticidad e integridad[202].

La decisión del legislador de delegar en el juez de instrucción la determinación de la manera en que va a llevarse a cabo la implementación de las medidas de investigación en cada caso concreto responde a la realidad imperante en materia tecnológica, conforme la cual el ritmo vertiginoso de la evolución en los dispositivos, las aplicaciones y el *software* torna imposible una regulación detallada sobre el particular. En tal contexto, es responsabilidad de los jueces evaluar el modo en que pueden utilizarse las herramientas disponibles (en especial, en cuanto es materia de este trabajo, el uso de *spyware*) adecuándolo a las circunstancias que se derivan de la citada evolución (tanto en lo tocante a las características de los recursos a su disposición como a la de las contramedidas tecnológicas en manos de los ciudadanos). Esto demanda a los magistrados un compromiso mucho mayor, puesto que ya no pueden limitarse a evaluar simplemente si la medida es procedente o no, sino que deben analizar el impacto del recurso a cada técnica en particular sobre los derechos de los investigados en el caso específico en que les toca participar, a la luz de los parámetros establecidos en la LEC en materia de proporcionalidad.

En los EE.UU., la legitimidad de este tipo de delegación legislativa ha sido objeto de controversia tanto en la doctrina como en la jurisprudencia. Por un lado, desde un sector se considera evidente que los tribunales se encuentran en mejor posición que el Congreso para

[199] En efecto, sobre el principio de proporcionalidad existe una muy consolidada doctrina del Tribunal Constitucional que distingue tres aspectos o vertientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) (STC 43/2014, de 27 de marzo; STC 23/2014, de 13 de febrero; STC 16/2014, de 30 de enero; STC 199/2013, de 5 de diciembre y STC 173/2011, de 7 de noviembre, entre otras). Cfr. VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", cit., pág. 14.

[200] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 16.

[201] Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit.

[202] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., págs. 27/28.

crear (jurisprudencialmente) un conjunto de reglas que balanceen en forma efectiva los intereses en juego (efectividad vs. privacidad o intimidad)[203]. En sentido opuesto, la Corte Federal de Apelaciones del 4° Circuito enfatizó que, en atención a dichas circunstancias, la responsabilidad principal de evaluar su impacto en el derecho a la privacidad y de actualizar la legislación recae en el poder del Estado al que se le confirió la facultad de tomar esas decisiones: el legislativo[204].

Si bien, por mi parte, considero que, por los motivos señalados precedentemente, la regulación legislativa precisa del uso de este tipo de herramientas informáticas de investigación no es factible en la práctica, es forzoso reconocer que la delegación de la implementación en los jueces enfrenta un problema serio: que *requiere, como mínimo, un conocimiento básico de cómo funcionan las herramientas informáticas* utilizadas. Sin embargo, la realidad es que la formación de los jueces no los torna aptos, '*per se*', para evaluar cuestiones complejas de ciencia informática, y por ende están mal equipados para decidir en los casos que involucren el uso de estas tecnologías[205]. En este marco, queda claro que la capacitación en la materia tecnológica y la posibilidad de contar con la asistencia de expertos en caso de necesidad será esencial para que los magistrados puedan hacer las preguntas correctas y detectar la presencia de irregularidades[206].

Es menester tener presente, al respecto, que la experiencia que puedan tener los jueces intervinientes en materia de investigaciones en el mundo *físico* resulta de muy poca utilidad para evaluar adecuadamente lo tocante a la proporcionalidad o idoneidad de las medidas en el mundo virtual, toda vez que la naturaleza de la evidencia digital y de las herramientas para obtenerla es radicalmente diferente a la de su contraparte física[207]. Por consiguiente, para valorar -por ejemplo- la proporcionalidad del registro remoto de un ordenador y la aprehensión de los datos electrónicos, no pueden aplicarse los mismos parámetros que se utilizan en relación con los registros domiciliarios y la incautación de documentos[208]. Ello, toda vez que -a menos que la herramienta sea especialmente programada para buscar sólo los archivos que

[203] En tal sentido: SOLOVE, Daniel J. (2005): "Fourth Amendment codification and Professor Kerr's misguided call for judicial deference", en *Fordham Law Review*, Vol. 74, N° 2, págs. 747/777; y, más recientemente, SKLANSKY, David Alan (2015): "Two more ways not to think about privacy and the Fourth Amendment", en *University of Chicago Law Review*, Vol. 82, N° 1, págs. 223/242.

[204] Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., pág. 42. La posición del tribunal citado es secundada, en la doctrina, por Orin S. KERR (2004): "The Fourth Amendment and new technologies: Constitutional myths and the case for caution", en *Michigan Law Review*, Vol 102, N° 5 págs. 801/888. Del mismo autor, en respuesta a las críticas de Daniel SOLOVE: (2005) "Congress, the courts, and new technologies: A response to Professor Solove", en *Fordham Law Review*, Vol. 72, N° 2, págs. 779/790.

[205] Al respecto, GHAPPOUR cita la opinión de un ex magistrado que señaló que los "…jueces que no están al día con los avances tecnológicos no le hacen ningún favor al público. La persecución penal ha evolucionado, y es difícil ponerle freno a los excesos si no se entienden las cuestiones en juego" (Cfr. GHAPPOUR, Ahmed (2017): "Searching places unknown: Law enforcement jurisdiction on the dark web", en Stanford Law Review, Vol. 69, N° 4, págs. 1134/1135). Destacó también que para que el proceso le pueda ser correctamente explicado al juez a fin de adoptar una decisión informada, esto requiere que el magistrado sepa que es lo que tiene que preguntar (Ibídem, pág. 1114, nota § 196. Con cita de CUSHING, Tim (2015): "Judge John Facciola on today's law enforcement: I'd go weeks without seeing a warrant for anything 'tactile'", en TECHDIRT, publicado el 3/3/2015; y NAKASHIMA, Ellen (2015): "Meet the woman in charge of the FBI's most controversial high-tech tools", en The Washington Post, publicado el 8/12/2015.

[206] Cfr. GHAPPOUR, Ahmed (2017): "Searching places unknown…", cit., págs. 1134/1135 (énfasis añadido).

[207] En profundidad, sobre esta cuestión, ver KERR, Orin S. (2005): "Digital evidence and the new criminal procedure", en *Columbia Law Review*, Vol. 105, N° 1, págs. 299/306.

[208] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 31.

respondan a determinados criterios- una vez ejecutado, el *spyware* estatal será capaz de recolectar todos los archivos almacenados en un determinado equipo, estén o no relacionados con la pesquisa, incluyendo los que se refieren a terceros inocentes[209]. De allí que algunos expertos, a efectos de ilustrar el grado de intrusión a la privacidad que puede generarse mediante el acceso a un sistema informático, han comparado la situación con un allanamiento físico en el que se secuestra *la totalidad del contenido de una vivienda*, y no sólo los elementos que pueden servir como evidencia de un ilícito específico[210].

En ese orden de ideas, BACHMAIER WINTER advierte, con acierto, que cuando del uso de herramientas informáticas se trata, el principio de proporcionalidad puede lesionarse tanto en el momento de proceder a la autorización de la medida *como en la fase de ejecutarla*. Sin embargo, en lo que respecta a esta última fase poco o nada se especifica en la ley: todo ha de ser definido y delimitado en la resolución judicial *ad hoc*, pero no se ofrece a los jueces de instrucción pautas que les indiquen cómo delimitar esa ejecución para que sea respetuosa con el principio de proporcionalidad. Al mismo tiempo, es importante recordar la volatilidad de los datos electrónicos, lo cual obliga a adoptar rápidamente medidas de conservación de los datos para evitar su destrucción. Como consecuencia, ha de descartarse la posibilidad de que los agentes al cargo del registro remoto realicen un filtrado minucioso de los datos relevantes antes de proceder a copiar los archivos. El proceso de ordinario tendrá lugar a la inversa: primero se procederá a clonar el contenido y después se seleccionarán los datos relevantes para la investigación, sin que previamente queden eliminados de esa aprehensión datos que afecten al núcleo de la intimidad del individuo[211].

La divergencia fundamental entre el registro físico y el digital, y las dificultades que la misma entraña al momento de fijar los parámetros para una medida de investigación realizada mediante herramientas informáticas, quedó evidenciada en uno de los primeros casos jurisprudenciales involucrando el uso de spyware. En efecto, en el caso "Scarfo", en los EE.UU., la discusión giró en torno a la legitimidad del registro efectuado por el FBI en el ordenador del sospechoso, oportunidad en la que utilizó un programa *keylogger* para obtener la contraseña necesaria para poder acceder a un archivo encriptado, almacenado dentro de ese mismo ordenador.

En tal contexto, el tribunal interviniente rechazó una moción de nulidad interpuesta por la defensa de Scarfo, que argumentó que la circunstancia de que el programa registrara *todo* lo

[209] Cfr. OWSLEY, Brian L. (2015): "Beware of government agents bearing trojan horses", en *Akron Law Journal*, Vol. 48, N° 2, pág. 344.

[210] Cfr. TIMBERG, Craig / NAKASHIMA, Ellen (2013): "FBI's search for 'Mo', suspect in bomb threats, highlights use of malware for surveillance", en *The Washington Post*, 6/12/2013, obtenido en: https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html..

[211] Por eso mismo, en la materia tampoco resultan de utilidad, como parámetros, los criterios establecidos por el TEDH para los allanamientos a domicilios físicos. Valga como ejemplo lo resuelto por el mencionado tribunal en la STEDH *Niemietz v Germany*, de 16 de diciembre de 1992 (Appl. N.º 13710/88), en la que se estableció que se había vulnerado el art. 8 del CEDH en el registro del despacho profesional de un abogado, por haberse aprehendido un número elevado de carpetas no relacionadas con el delito ni relevantes para la investigación. La imposibilidad de trasladar ese criterio a un registro informático, en el cual -en especial si es remoto y subrepticio- resulta esencial recolectar todo el contenido lo antes posible para evitar que sea eliminado o alterado, para recién después filtrar su contenido en busca de la evidencia relevante, deviene evidente.

que se tecleaba en el ordenador (y no únicamente la contraseña que la medida apuntaba a obtener) tornaba irrazonable el registro. En sustento de su decisión de desestimar dicha moción, el tribunal recurrió a la comparación con los allanamientos de morada, explicando que cuando estos últimos se llevan a cabo, las fuerzas de seguridad a menudo desconocen cuál es la evidencia incriminatoria hasta que no se topan con la misma, lo cual conlleva que se revisen muchas cosas irrelevantes hasta dar con las que sí lo son[212]. En igual sentido, destacó que la 4ª Enmienda de la Constitución de los EE.UU. no invalida un registro por el sólo hecho de que no pueda ser realizado con "precisión quirúrgica"[213]. Por consiguiente, cuándo la obtención de evidencia depende del análisis de documentos o claves informáticas cuya naturaleza precisa no puede saberse de antemano, se debe otorgar a las fuerzas de seguridad cierto margen para revisar el cúmulo de información existente en el sitio a fin de identificar la que se menciona en la orden judicial[214].

Sin embargo, la argumentación del tribunal fue criticada por un sector de la doctrina, que consideró inaplicable la comparación efectuada por los magistrados entre el uso del *spyware* en el caso y la revisión de un fichero físico en busca de un documento específico, destacando que al disponerse la medida no se había establecido previamente cuáles eran las combinaciones de teclas que se consideraban relevantes y debían ser "secuestradas" ("*seized*"), sino que permitió obtener la totalidad de la información para luego identificar lo que fuera de interés para la investigación[215].

En realidad, el fallo de ambos argumentos (el del tribunal y el de la autora que lo critica) reside en intentar equiparar el registro informático con el registro físico de una vivienda, cuando por su naturaleza, estas medidas son radicalmente diferentes. A lo que cabe añadir que, en el caso concreto analizado, en el que lo que se llevó a cabo es un registro *prospectivo* (toda vez que no estaba dirigido a recolectar evidencia que el sospechoso ya tenía almacenada, sino una que iba a producir en el futuro: la contraseña para el archivo encriptado) el modo en que se empleó el *spyware* se asemeja más a una intervención telefónica que a un allanamiento. Ello, desde que -tal como ocurre en la interceptación de las comunicaciones- aun conociendo de antemano que es lo que se *pretende* obtener (justificación de la medida) es imposible saber qué es lo que se *va* a obtener. Por ende, la medida –por su propia naturaleza- habrá de capturar información irrelevante (que puede ser sensible, o estar protegida por el secreto profesional) *junto a la que resulta relevante* para la investigación, lo cual obliga a diferenciar una de otra sólo después de haberla obtenido.

---

[212] *United States v. Nicodemo S. Scarfo*, 180 F. Supp. 2d 572, 581–82 (Corte de Apelaciones del Distrito de New Jersey, 2001). Con cita de fallos: *United States v. Conley*, 4 F.3d 1200, 1208 (Corte Federal de Apelaciones del 3er Circuito, 1993); *United States v. Carmany*, 901 F.2d 76 (Corte Federal de Apelaciones del 7° Circuito, 1990); *United States v. Fawole*, 785 F.2d 1141, 1145 (Corte Federal de Apelaciones del 4° Circuito, 1986); *United States v. Santarelli*, 778 F.2d 609, 615-16 (Corte Federal de Apelaciones del 11° Circuito, 1985); *United States v. Issacs*, 708 F.2d 1365, 1368-70 (Corte Federal de Apelaciones del 9° Circuito, 1983) y *United States v. Christine*, 687 F.2d 749, 760 (Corte Federal de Apelaciones del 3er Circuito, 1982).

[213] United States v. Nicodemo S. Scarfo, cit. Con cita de United States v. Conley.

[214] United States v. Nicodemo S. Scarfo, cit.

[215] Cfr. MURPHY, Angela (2002): "Cracking the code to privacy: How far can the FBI go?", en *Duke Law & Technology Review,* Vol. 1, pág. 5. Al respecto, la autora citada apunta que al instalar el *spyware* en el ordenador de Scarfo, el FBI no tenía modo de saber si el sospechoso iba a utilizar el teclado para introducir la contraseña del archivo encriptado o para escribir una nota a su abogado revelando información protegida por el secreto profesional.

Sentado cuanto precede, es preciso reconocer que, aunque esta regulación legal no merezca objeción alguna, es preciso atender a la circunstancia de que, en la práctica, y salvo excepciones, los jueces de instrucción no tienen conocimientos de informática suficientes para decidir cuál es el *software* que debe utilizarse para el registro remoto o cómo debe realizarse la copia y conservación de los datos que se aprehendan. En esa línea parece claro que hasta que los jueces de instrucción no reciban formación especializada en estas materias y se elabore un protocolo de ejecución de las medidas, habrán de confiar en las indicaciones que reciban de los propios agentes especializados en delitos telemáticos o en peritos informáticos[216]. A su vez, será responsabilidad de los agentes de la policía judicial que si cuenten con dichos conocimientos, procurar que en la aplicación en la que se solicite la medida se expliquen, de modo sucinto y comprensible para un lego en materia informática, las características y el funcionamiento de la herramienta informática que se pretenda utilizar, de modo que el magistrado pueda adoptar una decisión correcta sobre la cuestión.

9. El problema de la especificidad

El uso de medidas de investigación como las que vienen analizándose, en especial cuando se concretan mediante el recurso a programas espías, repercute directamente en dos cuestiones fundamentales vinculadas a la injerencia sobre el derecho a la intimidad amparado en el art. 18 de la CE y 8 del CEDH. Por un lado, el requisito de "especificidad" o "especialidad", entendido como la obligación de acotar el alcance de la medida solo a las personas y la información de interés para la investigación; por el otro, la minimización de sus efectos mediante la introducción de límites razonables en orden a su alcance y duración[217]. En atención a ello, el legislador ha incluido a la "especialidad" y la "idoneidad" entre los "principios rectores" mencionados en el art. 588 bis (a)(1).

En este orden de ideas, no puede pasarse por alto que la instalación del *spyware*, al llevarse a cabo en general en forma remota (a través de Internet), entraña de por si el riesgo de afectar a terceros, debido a la posibilidad de que el programa termine instalándose en un equipo equivocado. Sin embargo, este riesgo puede conjurarse adoptando medidas técnicas como por ejemplo encriptar el *spyware* de modo tal que solo pueda instalarse en el ordenador o sistema informático específico al que se refiere la autorización judicial[218]. Precisamente, la aclaración de que la herramienta informática ha sido programada de ese modo es una de las cuestiones que deberían ser informadas al magistrado interviniente de conformidad con lo establecido en el art. 588 bis (b)(6) de la LEC.

De todas maneras, la posibilidad de que la medida afecte a terceros ha sido expresamente prevista por el legislador en el art. 588 bis (h) de la LEC, sometiéndola a los límites introducidos en la reglamentación de cada una de las medidas incorporadas a través de la LO 13/2015, a los que cabe añadirle, desde luego, el análisis sobre la necesidad y proporcionalidad conforme lo dispuesto en el art. 588 bis (a), parágrafos §§ (4) y (5), tarea que debe concretar el juez de instrucción competente en base a las circunstancias particulares del caso concreto.

[216] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., págs. 27/28.
[217] Cfr. CARRELL, Nathan E.: "Spying on the mob…", cit., pág. 201.
[218] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2014): "Lawful hacking…", cit., págs. 39/40.

En tal contexto, la jurisprudencia de los países en los que esta clase de medidas viene aplicándose con cierta regularidad desde hace un tiempo ofrece ciertas pautas sobre los parámetros en los que se funda el análisis judicial con relación al principio de especificidad. Así, por ejemplo, en el marco de una impugnación contra el uso de un programa espía instalado en un teléfono móvil -fundada en la no introducción de límites a las comunicaciones que podían ser captadas por la herramienta informática-, la Corte Federal de Apelaciones del Distrito Sur de Nueva York estableció en el precedente *United States v. Tomero*[219] que el recurso al spyware resultaba legítimo por haberse acreditado la ineficacia de cualquier método alternativo para obtener la evidencia buscada y por haberse demostrado que las conversaciones a ser captadas involucraban a al menos uno de los individuos objeto de investigación[220]. Es decir que a partir de la ponderación entre la posible afectación a terceros inocentes y la utilidad potencial de la medida (utilizada en medio de una investigación contra el crimen organizado), se inclinó por considerarla válida.

Mucho más recientemente, empero, otro tribunal estadounidense adoptó la postura opuesta, aunque en este caso con relación a una medida mucho más intrusiva, como lo es sin duda la vigilancia audiovisual de una vivienda mediante el encendido remoto de la cámara web de un ordenador. Ello, toda vez que, en este supuesto, en la mayoría de los casos no puede saberse de antemano donde está ubicado el ordenador objeto de la medida -el que, además, si se trata de una laptop, puede ser cambiado de lugar por alguno de sus usuarios-, circunstancia que incrementa el peligro de que la vigilancia termine afectando a terceros completamente inocentes[221] o redunde en una injerencia sobre la intimidad de gran intensidad, del tipo que fue declarada inconstitucional por el VBerfG en el fallo reseñado *Supra*[222].

En atención a estas cuestiones, un Juez Federal de Cámara en el estado de Texas (EE.UU.) denegó, en 2013, el pedido del FBI de utilizar un programa informático para –entre otras cosas- encender remotamente la cámara web del sospechoso. En su fallo[223], el magistrado señaló que el pedido de la referida agencia federal no cumplía con los requisitos exigidos para la video vigilancia[224], destacando que la computadora objeto de la solicitud podía encontrarse tanto en una vivienda como en una biblioteca pública o en cualquier otro sitio. El juez tampoco aceptó la explicación del gobierno en punto a que el software estaba diseñado para capturar "sólo la información mínima necesaria para determinar la ubicación de la computadora e identificar al sospechoso", apuntando que el volumen de la información que el FBI pretendía obtener a

[219] 462 F. Supp. 2d 565 (2006). En la causa, el FBI requirió –y obtuvo- autorización judicial para usar "roving bugs" para escuchar las conversaciones de varios individuos vinculados con una familia mafiosa. De ese modo, se hizo de cientos de horas de grabación a través de la explotación de varios teléfonos celulares. El tribunal rechazó todas las objeciones planteadas por las defensas, dirigidas a excluir la evidencia obtenida del modo descripto.

[220] Cfr. JOYCE, Frederick M. / BIGART, Andrew E. (2007): "Liability for all, privacy for none: The conundrum of protecting privacy rights in a pervasively electronic world", en *Valparaiso University Law Review*, Vol. 41, N° 4, pág. 1504.

[221] Cfr. ANDREWS, Lori / HOLLOWAY, Michael / MASSOGLIA, Dan (2015): "Digital peepholes. Remote activation of webcams: Technology, law, and policy", *Institute for Science, Law and Technology*, ITT Chicago-Kent College of Law, pág. 13.

[222] Ver § 6.

[223] *In re*: *Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d at 755 (Corte Federal de Apelaciones del Distrito Sur de Texas, 2013).

[224] Cfr. ANDREWS, Lori / HOLLOWAY, Michael / MASSOGLIA, Dan (2015): "Digital peepholes…", cit., pág. 13.

través del spyware contradecía su afirmación de que la vigilancia pretendida iba a minimizarse[225].

En Italia, la Corte de Casación se pronunció en varias oportunidades sobre estas cuestiones. Inicialmente, en el caso "Musumeci" de 2015[226], el referido tribunal invocó el art. 8 de la CEDH para concluir que la activación remota de la videocámara y el micrófono de un ordenador por parte de las autoridades habían excedido la autorización normativa en la legislación local, toda vez que a través del *software* se había concretado una intrusión sin limitación alguna en términos de tiempo o locación. De todos modos, el tribunal no prohibió dicha práctica, sino que estableció que para ejecutar legítimamente una "interceptación invasiva" las autoridades debían obtener previa autorización judicial especificando cuándo y dónde iba a tener lugar la misma[227].

No obstante ello, tan sólo un año más tarde[228], el pleno de la Corte de Casación ("*Sezione Unite*") flexibilizó dicha postura, señalando que podía autorizarse el uso de un troyano en el marco de investigaciones por delitos graves (por ejemplo, involucrando terrorismo o crimen organizado) dentro de residencias privadas *incluso sin autorización judicial previa* y sin que mediare certeza sobre la efectiva comisión de un delito en el momento de la interceptación[229]. En sustento de dicha decisión, la Corte de Casación expresó que la Constitución Italiana no contiene una prohibición absoluta respecto de la interceptación de comunicaciones en el interior de lugares privados, indicando asimismo que la jurisprudencia del tribunal estableció que los derechos fundamentales previstos en los arts. 14 y 15 de la Constitución de ese país se preservan mediante la exigencia de autorización judicial previa en orden al inicio y las modalidades de la interceptación. El tribunal añadió que la exigencia de que se especifique la locación precisa en que va a llevarse a cabo la interceptación no se encuentra expresamente prevista ni en el Código de Procedimientos italiano ni en la jurisprudencia del TEDH, y tampoco puede ser considerada como un requisito para la validez de la interceptación, dado que se trata de una cuestión vinculada al modo en que la misma va a llevarse a cabo (por consiguiente, es exigible -por ejemplo- si la escucha se va a ejecutar por medio de la instalación de micrófonos ocultos, pero no cuando se concreta a través de un virus informático, supuesto en que se configura una interceptación "móvil")[230].

Los mencionados requisitos si son exigidos por la LEC, de conformidad con las disposiciones introducidas en la LO 13/2015, Así ocurre con respecto al acceso remoto a sistemas informáticos en el art. 588 septies (a)(2)(a) y en lo tocante al monitoreo de comunicaciones en

[225] Cfr. ANDREWS, Lori / HOLLOWAY, Michael / MASSOGLIA, Dan (2015): "Digital peepholes…", cit., pág. 16.
[226] Suprema Corte de Casación, Sentencia 27100 (caso "Musumeci"), del 26/5/2015.
[227] Cfr. DE ZAN, Tomasso (2016): "E-evidence and cross border data…", cit., págs. 47/48.
[228] Suprema Corte de Casación, caso 6889/2016, rta. el 28/4/19.
[229] Cfr. DE ZAN, Tomasso (2016): "E-evidence and cross border data…", cit., pág. 48 (énfasis añadido).
[230] Cfr. Eurojust (2016): "Cybercrime Judicial Monitor", Eurojust Limited, N° 2, pág. 17. Con relación al precedente dictado en 2015 en el caso "Musumeci", el pleno de la Corte de Casación refirió que en dicho fallo no se habían tomado en consideración la clara distinción legal prevista en la legislación entre la interceptación de comunicaciones entre personas presentes en una locación *determinada*, y la de personas presentes en sitios privados (indeterminados), ni el régimen especial establecido en la Ley 152 (referida a la persecución del crimen organizado). Por tales motivos, se había apartado de la jurisprudencia del tribunal que legitimó el uso de virus informáticos en investigaciones vinculadas a la criminalidad organizada sin exigir la previa identificación de las locaciones en las que iba a concretarse la interceptación.

el art. 588 ter (b)(1). Por añadidura, el art. 588 bis (b)(3) establece en general que la solicitud de autorización judicial de cualquiera de las medidas tecnológicas debe contener "[l]*os datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida*"[231].

En los EE.UU., el cumplimiento de estos requisitos, estrechamente vinculados con el principio de especificidad, ha generado un intenso debate doctrinario y jurisprudencial en relación con la concreción, por parte del FBI, de varias operaciones bajo la modalidad de "ataque de abrevadero", que culminaron en registros masivos a partir de autorizaciones judiciales impartidas sin que estuviesen claras, en el momento de emitirse, ni la identidad de los sospechosos ni la de los ordenadores objeto de la medida[232]. En efecto, en estos supuestos, la circunstancia de que, al momento de autorizar el uso del *spyware*, el juez competente desconozca en qué equipo va a introducirse el *software* espía ni a quién le pertenece -dado que el propósito del ataque informático es, precisamente, el de identificar al ordenador y a su dueño- deriva en un problema aparentemente insoluble a la hora de cumplir con el requisito de especificidad.

En busca de una solución, un sector de la doctrina estadounidense se apoya en que la Suprema Corte de ese país ha establecido, en el precedente *United States v. Karo*[233], que el requisito de especificidad podía sortearse cuando el propósito del registro inicial es determinar cuál es el área de búsqueda. En esa dirección, MAYER[234] entiende que la mejor solución reside en la doctrina de las "ordenes anticipadas" ("*anticipatory warrants*")[235], cuya constitucionalidad también fue ratificada por la Suprema Corte[236]. Explica, al respecto, que los tribunales estadounidenses vienen permitiendo desde hace largo tiempo registros y arrestos sometidos a ciertas condiciones que habilitan su ejecución. La premisa es que las cortes pueden identificar previamente ciertos hechos que pueden probablemente ocurrir y que, en tal caso, satisfacen el requisito de particularidad y sospecha razonable ("*probable cause*"). Una vez autorizadas, las fuerzas de seguridad esperan a que efectivamente ocurran los hechos que condicionan la legitimidad de la autorización judicial y luego ejecutan la medida autorizada. Ello ocurre, por ejemplo, con la entrega controlada, en la que se condiciona el registro a la recepción de un determinado "paquete", que en el momento de dictarse la orden no se sabe a ciencia cierta si va a ser recibido o no, y en algunos supuestos tampoco quién va a recibirlo o donde[237].

En los "ataques de abrevadero", el accionar estatal se rige por los mismos principios. Lo que se sabe de antemano es que existe una página web (la que se "infecta" con el *spyware* estatal) que

---

[231] Énfasis añadido.
[232] Cfr. BELLOVIN, Steven M. / BLAZE, Matt / LANDAU, Susan (2016): "Insecure surveillance…", cit., pág. 19.
[233] 468 U.S. 705, 718 (1984).
[234] Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., pág. 58.
[235] Son aquellas que se basan en la demostración de una sospecha razonable consistente en que en un momento futuro (pero no en el momento en que se libra la orden) cierta evidencia de un delito va a estar presente en un lugar determinado. Al respecto, se explica que las órdenes anticipatorias requieren que el magistrado que las emite determine que: (1) es probable que (2) contrabando, o evidencia de un delito, o un fugitivo puedan encontrarse en el lugar (3) cuando la orden se ejecute (Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., pág. 58, con cita de *United States v. Garcia*, 882 F.2d 699, 701-04, Corte Federal de Apelaciones del 2° Circuito, 1989 y *United States v. Grubbs*, 547 U.S. 90, Corte Federal de Apelaciones del 2° Circuito, 2006).
[236] In re: United States v. Grubbs, 547 US 90, 94 (2006).
[237] Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., pág. 58.

contiene contenidos ilícitos, a la cual habrán de acceder usuarios cuya identidad se desconoce, a través de ordenadores también desconocidos, para descargar ilegalmente los referidos contenidos. Esto es: pueden identificar una serie de circunstancias que, en caso de verificarse, determinan que exista una alta probabilidad de que el programa espía habrá de introducirse en los ordenadores de sujetos respecto de los cuales se cumplen los requisitos de especificidad y sospecha razonable de la comisión de un delito (puntualmente, la descarga de contenidos ilícitos mediante Internet)[238]. En tal supuesto, lo que se prevé en la orden judicial es la autorización para instalar el *spyware* estatal en los ordenadores de todos aquellos que se conecten con una página web específica y descarguen determinados archivos (por ejemplo, conteniendo imágenes de explotación sexual infantil), dado que existen motivos suficientes para sospechar la comisión de un delito en orden a todos esos individuos, aunque no se sepa quiénes son, ni qué ordenador están utilizando.

Con relación a ello, HENNESEY afirma que la autorización judicial impartida en el caso "Playpen" no sólo demuestra que se puede llevar adelante ataques "*watering hole*" cumpliendo con los requisitos constitucionales, sino que las referidas órdenes pueden cumplirse de un modo que asegura una protección especialmente eficaz de las garantías constitucionales. Explica, en tal sentido, que en estos casos el cumplimiento del requisito de especificidad es inusualmente robusto porque al acceder a la página y descargar material ilícito (imágenes de explotación sexual infantil) el usuario, de hecho, ya *ha consumado el delito* que se investiga[239].

10. Derecho de defensa vs. confidencialidad de la herramienta informática

Por su propia naturaleza, las medidas analizadas en el presente trabajo deben ser ejecutadas en forma subrepticia, toda vez que no pueden arrojar resultados satisfactorios si el sospechoso sabe que está siendo vigilado. En atención a ello, el art. 588 bis (d) de la LEC establece que tanto la solicitud como las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa. Al respecto, CASANOVA MARTÍ explica que el hecho que las medidas se practiquen en secreto no afecta al derecho de defensa, ya que éste podrá ejercitarse plenamente cuando finalice la intervención, momento en el que la parte afectada tiene la facultad de controlar el contenido de la misma[240].

A tal efecto, la LEC regula en el art. 588 ter (i) el acceso de las partes a las grabaciones, además de incorporar disposiciones vinculadas al control judicial sobre la ejecución de las medidas[241] y a las salvaguardas que deben adoptarse a fin de garantizar la "cadena de custodia" de los datos obtenidos y su confiabilidad tanto en el art. 588 ter (f) como en el 588 septies (a)(2)(e).

Ahora bien: cuando la medida involucra el uso de un *spyware* para obtener la evidencia digital, surge como cuestión estrechamente ligada a la de la cadena de custodia y el control sobre la confiabilidad y autenticidad de la evidencia colectada la de la posibilidad de la defensa de verificar *como fue obtenida* dicha evidencia, a cuyo efecto podría considerarse que es necesario que dicha parte *conozca cómo funciona el software utilizado* por el Estado para recogerla.

[238] Cfr. MAYER, Jonathan (2016): "Constitutional malware", cit., pág. 59.
[239] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., pág. 19 (énfasis añadido).
[240] Cfr. CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones…", cit.
[241] Previsto en general en el art. 588 bis (g) de la LEC.

Cuestión que plantea un conflicto entre la necesidad del Estado de ser eficiente en la persecución de los delitos y el de los particulares en ver resguardados sus derechos. Ello, desde que, por un lado, parece evidente que para una persona sometida a proceso en base a evidencia obtenida mediante el recurso a un programa espía, resulta esencial el acceso a la información respecto al funcionamiento de dicha herramienta informática para poder evaluar su confiabilidad, lo que implica que en el supuesto de que se le oculte el uso de *malware* (o en su caso, las características de dicho *malware*), se estaría vulnerando su derecho de defensa[242]. Mientras que, por el otro, es igual de evidente que si se obliga a las autoridades estatales a revelar cómo funciona el programa espía, se estaría comprometiendo la posibilidad de volver a emplearlo eficientemente en el futuro, reduciendo su -de por sí breve- vida útil[243]. A lo que se viene a sumarse, además, el riesgo de proliferación del *software* malicioso[244].

En atención a esto último, los gobiernos que utilizan *spyware* como medida de investigación hacen enormes esfuerzos para evitar que se divulguen las características de dichas herramientas, lo que ha generado conflictos entre las autoridades y los encausados en derredor del derecho de la parte a controlar la prueba de cargo, como derivación del derecho de defensa en juicio. Así, en los EE.UU., el tribunal de apelaciones que entendió en el caso "Scarfo" reseñado *supra*[245], rechazó el pedido de la defensa de obtener información detallada sobre el funcionamiento del sistema "*keylogger*" utilizado por el FBI[246]. La Fiscalía se había opuesto a la moción de la defensa invocando la "Ley de Procedimientos para Información Confidencial" ("*Classified Information Procedures Act*" o CIPA) de ese país, que autoriza a las autoridades gubernamentales a no divulgar datos confidenciales y aportar sólo información limitada a las defensas en ciertos casos[247]. En su lugar, aportó un sumario conteniendo una explicación genérica sobre el funcionamiento del programa, pero sin incluir ningún dato específico sobre sus características técnicas. El tribunal consideró que bastaba con la presentación del referido sumario[248].

En el régimen establecido para la adopción de estas medidas en la LEC -a partir de la reforma operada en la LO 13/2015, se advierte que la regla general sobre el contenido de las autorizaciones judiciales incorporada en el art. 588 bis (c) no prevé que el juez deba indicar la

---

[242] Cfr. SILVA RAMALHO, David (2014): "The use of malware…", cit., pág. 75.

[243] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., pág. 23. Cabe tener presente, al respecto, que las herramientas de hackeo son esencialmente perecederas; las actualizaciones de seguridad o la aparición de nuevas tecnologías las tornan obsoletas con regularidad.

[244] El riesgo de difusión y proliferación de vulnerabilidades y *exploits es inherente a su uso*. Ello es así debido a la naturaleza de estas verdaderas "ciberarmas" a las que el Estado recurre para penetrar los sistemas informáticos, las cuales -a diferencia de las armas convencionales- no explotan ni son destruidas al momento del impacto, sino que infectan en forma permanente su objetivo, donde pueden subsistir por días o años. Está claro que ello supone, en consecuencia, la posibilidad concreta de que un criminal técnicamente avanzado que note la existencia del *spyware* estatal en su equipo *pueda utilizar ingeniería inversa para conocer el código* y utilizarlo contra el propio Estado o en perjuicio de terceros inocentes (Cfr. GHAPPOUR, Ahmed (2017): "Searching places unknown…", cit., pág. 1111. Énfasis añadido). Lo cual conduce a otra diferencia entre estas ciberarmas y las convencionales. A diferencia de una herramienta física, estas herramientas digitales no pueden ser recuperadas. Una vez que una ciberarma está "libre", puede propagarse por el mundo en segundos, para ser utilizada por quien sea que la obtenga (WikiLeaks: "Press release: Vault 7", publicada el 7/3/2017).

[245] § 4.

[246] Cfr. MURPHY, Angela (2002): "Cracking the code to privacy…", cit., pág. 1.

[247] Cfr. AUCOIN, Kaleigh E. (2018): "The spider's parlour…", cit., pág. 1444.

[248] Cfr. CARRELL, Nathan E. (2002): "Spying on the mob…", cit., pág. 200.

descripción del modo en que la medida va a llevarse a cabo, aunque si se exige dicha precisión en la solicitud de la policía judicial o el Ministerio Fiscal, circunstancia que podría interpretarse como el reflejo de la intención del legislador de mantener en reserva los métodos utilizados para llevar a cabo las medidas de investigación. Sin embargo, en sentido opuesto, puede apreciarse que, al regular la medida de localización y rastreo, en el art. 588 quinquies (b)(2) se dispuso que la autorización debe especificar el medio técnico que va a ser utilizado; mientras que en lo tocante al el acceso remoto a un sistema informático se estableció en el art. 588 septies (a)(2)(b) que en la orden judicial se debe precisar el alcance de la medida "*…el software mediante el que se ejecutará el control de la información*".

Al respecto, cabe señalar que -en especial- la redacción de esta última disposición habilita el recurso a una solución que permite alcanzar cierto balance entre los intereses en juego, y que consiste en el diseño del *spyware* estatal bajo el modelo "lanzador/carga". Ello supone utilizar un programa separado en dos módulos, conforme lo cual por un lado se encuentra el software encargado de llevar a cabo la intrusión en el sistema objetivo (denominado "lanzador" o "*dropper*") y por otro el que obtiene la evidencia digital (al que se alude como la "carga" o "*payload*"). Ello, aprovechando que, a los efectos de la cadena de custodia y la confiabilidad de la evidencia recolectada, *sólo las características de este último programa resultan relevantes* para la defensa, a lo que se suma que -dado que se trata de un *software* "genérico", que no depende del uso de una vulnerabilidad para funcionar- su código puede divulgarse sin comprometer la efectividad de futuras interceptaciones ni aumentar el riesgo de proliferación. El código del *software* "penetrador", en cambio, puede mantenerse en reserva, ya que -por un lado- su funcionamiento no incide sobre la integridad y autenticidad de los datos informáticos que recolecta el programa principal y -por el otro- su divulgación sería perjudicial para el Estado (disminuyendo su capacidad para interceptar comunicaciones) y el público (debido a la proliferación de *exploits* peligrosos para la seguridad informática) sin generar como contrapartida un beneficio para el derecho de defensa y el debido proceso[249].

De conformidad con lo expuesto, y volviendo a lo establecido en la LEC, puede razonablemente interpretarse que cuando el legislador dispuso que debe identificarse el "medio técnico" para llevar a cabo la medida de rastreo o localización en el art. 588 quinquies (b)(2) o precisar cuál va a ser el *software* mediante el que se ejecutará el *control de la información* en el art. 588 septies (a)(2)(b) se refiere al programa en el módulo de "carga", y no al módulo que contiene la herramienta para lograr la intrusión. De este modo, se garantiza el derecho del encausado a controlar la cadena de custodia y la confiabilidad de la evidencia digital recogida en la investigación, sin comprometer la facultad estatal de persistir en el uso de la herramienta empleada en el caso ni poner en peligro la seguridad informática.

Esta fue, además, la postura adoptada por los representantes del gobierno de EE.UU. -con suerte disímil- en dos incidentes suscitados ante el mismo juez el marco del caso "Playpen", en los que las defensas habían peticionado que se les permitiese conocer cómo funcionaba el *spyware* utilizado para obtener la evidencia de cargo o, en su defecto, que se desestimara la acusación en su contra. Frente a ello, el FBI aceptó poner en conocimiento el módulo de "carga", pero no el "lanzador", mientras que la defensa solicitó acceder al código de ambas

[249] Sin embargo, algunos autores no admiten que el Estado pueda mantener el secreto sobre el malware utilizado en ningún caso. Ver, al respecto: CARRELL, Nathan E. (2002): "Spying on the mob…", cit., págs. 207/208.

partes de la herramienta informática estatal, alegando que poder defenderse necesitaban saber cómo había hecho el FBI para intrusar la computadora de sus clientes. En el primer caso, *Michaud*, el juez le dio la razón a la defensa (y en consecuencia, el fiscal levantó los cargos). Sin embargo, unos meses después, el mismo magistrado, fallando simultáneamente en tres incidentes acumulados - *Tippens, Lesan* y *Lorente*- resolvió en favor del gobierno[250].

El cambio de postura del juez en estos casos puso de resalto, según explica HENNESEY, la importancia de que los acusadores se encuentren en condiciones de transmitirle eficazmente al magistrado las cuestiones técnicas involucradas en la decisión que debe adoptar. Así, en el primer caso, frente al desconocimiento sobre cómo funcionaba la herramienta informática utilizada por el FBI, el juez se inclinó por los argumentos de la defensa en orden a la necesidad de conocer el código de la herramienta de intrusión. El análisis posterior sobre el caso por parte de expertos legales e incluso por la empresa Mozilla -autora del código explotado por el gobierno para introducir el *malware*- dejó en claro que el contenido de dicho programa solo hubiese sido relevante en caso de comprobarse que el FBI deliberadamente lo había programado para exceder el alcance de la autorización judicial. Basándose en ello, el juez enfrentó la siguiente serie de casos con más y mejor información, lo cual lo llevó a rechazar la pretensión de la defensa[251].

11. El problema de la aplicación trasnacional

Una última cuestión a considerar, en orden al acceso subrepticio estatal a los equipos o sistemas informáticos de los ciudadanos con autorización judicial, es la que se vincula con la posibilidad de que la medida rebase los límites de la jurisdicción del juez que la ordena o incluso los de la normativa procesal nacional en la que encuentra amparo. Ello, desde que en muchos casos, la circunstancia de que la intrusión al sistema informático del sospechoso se concrete de modo remoto a través de la Internet, determina que no pueda saberse, al momento de llevarla a cabo (o en el transcurso de la ejecución de la medida) si el dispositivo que contiene a dicho sistema (ya sea que se trate de un smartphone, un ordenador portátil o un servidor externo) se encuentra, o no, dentro de la jurisdicción del juez de instrucción que tiene a cargo la investigación. Por consiguiente, el recurso a estas herramientas de investigación puede plantear serios problemas en cuanto a su alcance transnacional[252].

Al respecto, BACHMAIER WINTER apunta, con acierto, que una de las cuestiones a las que habrán de enfrentarse los jueces a la hora de acordar el registro remoto de equipos informáticos es la de la localización de los datos electrónicos. Por ejemplo, cuando aquellos no sean accesibles a través del registro directo del ordenador por encontrarse archivados en un equipo informático ubicado en el extranjero, o en la "nube"[253], o en servidores situados fuera de las fronteras

[250] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., págs. 24/25.
[251] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., págs. 25/26.
[252] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 4.
[253] La "computación en nube" –según la definición del Instituto Nacional de Estándares y Tecnología ("*National Institute of Standards and Technology*" o NIST) de los EEUU- supone "[u]*n modelo para permitir el acceso ubicuo, conveniente y a pedido mediante la Internet a un conjunto compartido de recursos informáticos configurable (vgr., redes, servidores, espacio de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y lanzados con un mínimo esfuerzo de administración e interacción del proveedor del servicio*".

nacionales (en uno o más servidores)[254]. Sin embargo, el problema no está limitado a la medida de acceso remoto a un sistema informático prevista en el art. 588 septies (a) de la LEC o al supuesto de "registro extendido" regulado en el art. 588 sexies (b), dado que en cualquier caso en que se disponga judicialmente la introducción remota de *spyware* en un dispositivo o sistema informático (sea para monitorear las comunicaciones de la persona que lo utiliza, para localizarlo o para rastrearlo), se estará produciendo una intrusión en su ámbito de intimidad que debe estar autorizada por la ley. Por consiguiente, es imprescindible determinar qué régimen legal se aplica (es decir, *el de qué país*) y si es posible que éste proyecte su influencia sobre sujetos que se encuentran en el extranjero.

En ese orden de ideas, es preciso tener presente que, en el plano del Derecho internacional, la regla es la aplicación del principio de territorialidad, según el cual -una vez establecida la ubicación de los datos- se le reconoce jurisdicción sobre los mismos al Estado en cuyo territorio se encuentren. Así las cosas, cualquier intento de recolectar información de un servidor ubicado dentro de un país extranjero sin el consentimiento de dicho Estado constituiría, en principio, una infracción al principio de integridad territorial y –en consecuencia- también al Derecho internacional[255].

Ahora bien: del propio planteamiento del principio de territorialidad se desprende la principal dificultad que surge cuando se intenta aplicar en forma estricta un principio estrechamente vinculado con el mundo *físico* en un ámbito tan distinto a aquél, como lo es el ciberespacio: la exigencia de certeza respecto del lugar en que se encuentran los datos. En efecto, se aprecia que, por ejemplo, en cuanto atañe a la "computación en nube", la referida exigencia choca con un aspecto técnico central del funcionamiento de esa clase de servicios, que es que la información almacenada en la nube es constantemente transferida entre los distintos servidores, desplazándose de un país a otro en cualquier momento. Además, los datos pueden ser copiados por motivos de seguridad y disponibilidad, y por ende encontrarse en múltiples locaciones ya sea dentro de un mismo país o en varios al mismo tiempo. A consecuencia de este y otros factores, incluso el proveedor del servicio puede desconocer donde se encuentra exactamente la información[256]. Por consiguiente, según SPOENLE es posible afirmar que la locación –como constante aplicable a todos los datos físicos y también a los intangibles desde el nacimiento de Internet- no cumple ninguna función en el contexto de la computación en nube[257].

---

[254] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 25.

[255] Cfr. KOOPS, Bert-Jaap / GOODWIN, Morag (2014): "Cyberspace, the cloud…", cit., pág. 21 (citas omitidas). Un enfoque alternativo admite también el reconocimiento del "principio de nacionalidad", según el cual podría establecerse la jurisdicción criminal a partir de la nacionalidad del infractor. VACIAGO apunta, sin embargo, que este principio impone ciertas restricciones, ya que -dado el carácter generalmente trasnacional de los ciberdelitos- el criminal bien puede ser extranjero. Por añadidura, los datos carecen de nacionalidad, ya que ésta es un atributo exclusivo de los individuos (Cfr. VACIAGO, Giuseppe (2001): "Remote forensics and cloud computing: An Italian and European legal overview", en *Digital Evidence and Electronic Signature Law Review*, Vol. 8, pág. 124).

[256] En orden a esta cuestión, WALDEN explica que puede ser posible para el proveedor establecer a través de herramientas de informática forense precisamente en qué máquinas residían los datos al momento de ser requeridos, pero lo más probable es que esto recién se sepa *después* de obtenerlos, antes que en forma previa (Cfr. WALDEN, Ian (2011): "Accessing data in the cloud: The long arm of the law enforcement agent", en *Queen Mary School of Law Legal Studies*, Research Paper N° 74/2011, pág. 4. Énfasis añadido).

[257] Cfr. SPOENLE, Jan (2010): "Cloud computing and cybercrime…", cit., pág. 5.

De igual manera, cuando se distribuye un programa espía desde un punto central a una cantidad no determinada de sospechosos no identificados -como ocurrió en los EE.UU en el caso "Playpen" y más recientemente, en el propio continente europeo, en la operación contra el sistema EncroChat- no hay forma de que el juez que dispone la medida sepa de antemano si los sujetos pasivos de la misma se encuentran, o no, dentro de su jurisdicción o incluso en el mismo país, toda vez que -a decir verdad- pueden encontrarse en cualquier lugar del mundo. Incluso en el supuesto de que se autorice la instalación remota de un *spyware* para monitorear las comunicaciones de un sujeto específico, lo cierto es que en muchos casos bien puede desconocerse donde está el sospechoso en el momento en que el programa ingresa a su teléfono móvil o su ordenador, como así tampoco impedir que se desplace llevándolos consigo fuera de la jurisdicción del juez durante el transcurso de la medida.

A ello se suma un segundo problema, también vinculado al principio de territorialidad y la movilidad de la evidencia informática que es la aparición de países que actúan como verdaderos "refugios de evidencia digital", ofreciendo servicios de "*bulletproof hosting*" (literalmente: "hospedaje a prueba de balas"). Se trata, básicamente, de una variante de los servicios de "*web hosting*" tradicionales (esto es: el ofrecimiento de *data centers* para alojar servidores dedicados, para basar en ellos páginas web o almacenar información digital), pero que a diferencia de los tradicionales no sólo no establecen ningún control sobre el contenido de las páginas web o datos que alojan, sino que enfatizan la circunstancia de que las leyes aplicables en esos países garantizan que aquellos estarán a salvo de cualquier pedido de cooperación internacional requiriendo que se dé de baja la página, se secuestren los datos o se brinde información sobre los clientes.

En tal contexto, surge el interrogante de si se lesiona el principio de territorialidad como resultado del acceso remoto a los datos almacenados en ordenadores o equipos ubicados fuera del territorio del país investigador y si, en su caso, dicha lesión considerarse justificada bajo ciertas circunstancias[258]. Interrogante que con toda seguridad está llamada a trasladarse del plano teórico doctrinario al judicial a partir de la operación concretada contra el sistema EncroChat. Ello, desde que en el caso, aunque la intrusión inicial a los efectos de introducir el programa espía estatal fue autorizada por un juez francés y llevada a cabo sobre un sistema ubicado en el territorio de ese país (en Niza), lo cierto es que desde allí el spyware se irradió a los sistemas operativos en los teléfonos *de todos los usuarios* de EncroChat, no sólo en Francia sino en toda Europa y también más allá[259]. Lo cual significa que, a partir de la autorización emitida por un magistrado francés con fundamento en la legislación procesal francesa, se produjo una injerencia en el derecho a la intimidad y al secreto de las comunicaciones de personas residentes en Holanda, Inglaterra y muchos otros países de Europa, en los que no rige aquella normativa.

En los EE.UU., la cuestión de si el juez puede válidamente autorizar una medida que proyecta sus efectos más allá de su jurisdicción territorial ocupó un lugar central en la discusión jurisprudencial en derredor del caso "Playpen", toda vez que las defensas de los imputados plantearon la nulidad de la autorización impartida por el juez federal interviniente, en tanto

[258] Cfr. Seitz, Nicolai (2005): "Transborder search: A new perspective in law enforcement?", en *Yale Journal of Law and Technology*, Vol. 7, N° 1, pág. 27.
[259] Cfr. Cox, Joseph (2020): "How police secretly took over a global pone network for organized crime", cit. (énfasis añadido).

autorizó al FBI a instalar un *spyware* en los ordenadores de personas ubicadas en distintos puntos de ese país y también en el extranjero, a pesar de que en la norma aplicable (art. 41 de las Reglas Federales de Procedimiento Criminal) se restringía la competencia para emitir órdenes de registro y secuestro ("*warrants*") *a los confines del distrito asignado al magistrado*[260]. Frente a ello, en el precedente dictado *in re*: *US v. Horton*[261], la Corte Federal de Apelaciones del 8° Circuito, aun admitiendo que la legislación procesal no autorizaba al magistrado a autorizar la medida tal cual la había solicitado el FBI, decidió no aplicar la regla de exclusión por entender que concurría la "excepción de buena fe" reconocida en el precedente *United States v. Leon* de la Suprema Corte de EE.UU.[262], según el cual la regla no debe aplicarse cuando los agentes de las fuerzas de seguridad actúan de buena fe y la infracción constitucional se debe a un error judicial[263].

Traída la cuestión al ámbito español, cabe preguntarse cómo debe proceder el juez de instrucción cuando se le plantea la posibilidad de autorizar una medida que tenga o pueda tener carácter trasnacional. ¿Puede otorgar la autorización sobre la base de que la legislación española no lo prohíbe expresamente? ¿O debe denegar el permiso en línea con los principios establecidos en el Convenio de Budapest, cuya normativa se refiere solo a la obligación de los estados de facilitar el acceso a los datos almacenados "en su territorio"?[264]. Al respecto, se apunta que la regulación de la LEC en materia de registro remoto de ordenadores mediante *spyware* resulta excesivamente parca y ambigua; circunstancia que quizás se origine en una decisión deliberada del legislador, a la espera de lo que puedan disponer futuros convenios internacionales o lo que se establezca en materia de procesos penales transnacionales en la Unión europea, como la directiva sobre la orden europea de Investigación[265].

En la normativa internacional, si bien no existe una prohibición expresa de las ciberoperaciones transfronterizas[266], tampoco se ha adoptado alguna regulación especial que las habilite específicamente. Así, aunque el art. 19(2) de la Convención de Budapest prevé la posibilidad de una "búsqueda extendida en la Red", establece expresamente que las computadoras a las que puede extenderse la búsqueda *también deben encontrarse dentro del territorio del país* cuyas agencias llevan a cabo la investigación. Esto es: no permite la búsqueda transfronteriza. Sin embargo, la idea de implementar estos medios de investigación se encuentra presente en recomendaciones y resoluciones adoptadas en el seno de la Unión Europea desde hace más de una década. En esta dirección, un documento publicado en 2008 por la UE con recomendaciones para combatir el ciberdelito incluía, entre otras cuestiones, un

[260] Si bien la norma contemplaba unas pocas excepciones, entre ellas no se encontraba el desconocimiento de la locación de evidencia informática. Estas incluían (1) si la propiedad o persona a ser requisada se encontraba en un territorio, posesión o "*Commonwealth*" controlado por los EE.UU.; (2) si el objeto de la búsqueda estaba dentro de una representación consultar de los EE.UU.; o (3) si el objeto de la búsqueda se encontraba en un terreno propiedad de -o alquilado por- los EE.UU. usado por diplomáticos de ese país. También en casos excepcionales vinculados a la prevención del terrorismo.

[261] No 16-3976 (2017).

[262] 468 U.S. 897 (1984).

[263] El razonamiento de la Suprema Corte de EEUU es que como en dicho supuesto no existe una inconducta policial cuya reiteración pueda ser "disuadida" ("*deterred*") mediante la exclusión, los beneficios (marginales o inexistentes) que se derivan de la supresión de la evidencia no justifican los costos derivados de dicha medida.

[264] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 25.

[265] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., pág. 26.

[266] Cfr. GHAPPOUR, Ahmed (2017): "Searching places unknown…", cit., pág. 1085 (citas omitidas).

llamamiento para que las agencias policiales de los estados miembros llevaran a cabo "registros remotos" en ordenadores. A su vez, una nota distribuida unos meses antes por la Presidencia del Consejo de Europa sobre la cuestión indicaba que había "proyectos ya existentes" que requerían "enfoques comunes", incluyendo a los "registros en ordenadores, que constituyen una cuestión delicada por su naturaleza transfronteriza"[267]. En dicha nota se basó la propuesta formal para las conclusiones del Consejo, que inicialmente hacía un llamamiento a adoptar "medidas para facilitar los registros remotos en ordenadores", para permitir "a los investigadores el acceso rápido a los datos". La versión final de las conclusiones del Consejo pedía que se "facilitaran las búsquedas remotas en la medida en que están autorizadas por la ley local, permitiendo a los equipos de investigación acceder rápidamente a la información, *con la autorización del país requerido*"[268].

Desde la sanción del Convenio de Budapest hasta la actualidad, se han venido analizando numerosas propuestas de reforma vinculadas a la cuestión de los registros transfronterizos, sin que hasta la fecha haya podido alcanzarse el consenso necesario para que fueran aprobadas. Así, por ejemplo, una de estas propuestas para un eventual protocolo adicional a la citada convención propiciaba habilitar el "*…acceso remoto sin consentimiento [del país donde se encuentran los datos] pero con credenciales legalmente obtenidas*"[269] (esto es: sin recurrir a un *spyware*). El elemento clave de esta propuesta era la *autorización*, entendiéndose que cuando se accede con las credenciales correctas el servidor responde conforme se supone que tiene que responder de acuerdo a su programación; mientras que cuando *se fuerza el ingreso* por medios técnicos, el servidor, aunque también responde de acuerdo a su programación (pues por definición, un ordenador sólo puede actuar como fue programado), no lo hace del modo en que se supone que tenía que responder[270]. El tratamiento diferenciado entre ambos supuestos deriva de que si bien en el primero también existe un cierto elemento de engaño (ya que el agente estatal se hace pasar por el verdadero usuario, invocando su nombre de usuario y contraseña), no se altera el normal funcionamiento del sistema; en cambio cuando se accede explotando una vulnerabilidad, ello involucra la manipulación del referido sistema de un modo que influye en su funcionamiento[271].

En la doctrina internacional, la opinión predominante sigue siendo que la búsqueda transfronteriza relativa a datos protegidos[272] no está permitida, porque lesiona el principio de territorialidad, toda vez que la autoriza el Estado afectado[273]. Lo cual importaría que el interrogante planteado respecto de cómo debe actuar el juez de instrucción debería ser respondido por la negativa en todos aquellos casos en los que la ley del Estado en el cual se

[267] En ese momento, se destacó que la referencia a "proyectos ya existentes" parecía implicar que las fuerzas de seguridad en al menos algunos estados de la UE *ya estaban llevando a cabo* búsquedas remotas transfronterizas en sistemas informáticos.
[268] Cfr. BRENNER, Susan W. (2012): "Law, dissonance, and remote computer searches", en *North Carolina Journal of Law & Technology*, Vol. 14, N° 1, págs. 82/83 (énfasis añadido).
[269] Cfr. O'FLOINN, Micheál (2013): "It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe", en *Computer Law & Security Review*, Vol. 29 (citado de documento informático. Énfasis añadido).
[270] Dicho más sencillamente: en el segundo supuesto se aprovecha la programación para "engañar" al servidor a fin de que actúe de un modo distinto al debido.
[271] Cfr. KOOPS, Bert-Jaap / GOODWIN, Morag (2014): "Cyberspace, the cloud…", cit., pág. 49.
[272] Es decir, excluyendo a los que provienen de "fuentes abiertas", como publicaciones voluntarias en medios de comunicación, redes sociales, etc.
[273] Cfr. SEITZ, Nicolai (2005): "Transborder search…", cit., pág. 39.

encuentran ubicados los datos no contemple la posibilidad de que autoridades extranjeras lleven a cabo registros remotos en su territorio. Ello, toda vez que siendo dicha medida ilícita en el estado de ejecución, la admisibilidad de la misma en el estado del fuero podría cuestionarse[274].

Frente a ello, el problema es que -como bien apunta BOJARSKI- en atención al carácter global del fenómeno del ciberdelito, resulta casi imposible remediarlo sin autorizar a las agencias de investigación a perseguir a los responsables más allá de las fronteras de un determinado Estado[275]. De allí que en los tribunales de distintas partes del globo aumenten los casos en los que las autoridades utilizan evidencia obtenida de manera transfronteriza en sus diversas normas sin una base normativa clara, y hayan comenzado a surgir, en la doctrina y la jurisprudencia, posturas que, con distintos argumentos, defienden la posibilidad de legitimar el acceso directo transfronterizo en determinadas circunstancias.

Así, por ejemplo, un enfoque doctrinario apunta a relativizar la aplicabilidad del principio de territorialidad en lo tocante a la búsqueda transfronteriza, enfocándose en el carácter "virtual" del acceso de un Estado a los datos ubicados en otro. En esta línea, KERR y MURPHY consideran razonable argumentar que el tipo de ejercicio de la jurisdicción al que se refiere la regla -es decir, el principio de no intervención- es el *envío físico* de agentes al territorio de otro Estado para arrestar a un sospechoso o llevar adelante una investigación penal, y no a una pesquisa informática, que no involucre el ingreso físico a otro país[276]. En España, VELASCO NÚÑEZ apunta que ni el fenómeno de la deslocalización (es decir, el hecho de que la energía y los paquetes de datos informáticos y telecomunicativos se producen en un punto geográfico que deja de estar geolocalizado de inmediato aunque lo gestione una operadora que sí lo esté) ni el de la transnacionalidad (la circulación de los datos a través del espacio de más de un Estado soberano) son variables que afecten a los derechos fundamentales, y por lo tanto a la licitud de la prueba a que se refiere el art. 11.1 de la Ley Orgánica del Poder Judicial[277]. En esa dirección, argumenta que la tutela de los derechos fundamentales no puede quedar a la decisión del gestor de un servicio informático sobre el lugar que elija para ubicar los medios técnicos desde los que lo presta, máxime cuando opera –y la infracción penal produce efectos dañinos– en el país que trata de perseguir el delito[278]. No obstante, desde la vereda de enfrente se objeta que un registro transfronterizo siempre genera cambios físicos perceptibles en el mundo exterior dentro del territorio del tercer país. Por consiguiente, es irrelevante si el oficial actuante esta físicamente presente en el lugar o si accede mediante la Internet. El resultado de su actividad es igual en ambos casos: se procesan datos en servidores ubicados en un territorio soberano extranjero[279].

[274] Cfr. BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos…", cit., págs. 26/27.
[275] Cfr. BOJARSKI, Kamil (2015): "Dealer, hacker, lawyer…", cit., pág. 40. No obstante, el propio autor reconoce que de esto se desprenden cuestiones graves concernientes a la protección de la privacidad y el abuso de poder, derivadas de la concesión de una facultad indiscriminada a las fuerzas de seguridad para introducirse en cualquier red informática del mundo a partir de una orden judicial local (ibídem).
[276] Cfr. KERR, Orin S. / MURPHY, Sean D. (2017): "Government hacking to light the dark web. What risks to international relations and international law?", en *Stanford Law Review Online*, Vol. 70, pág. 66 (énfasis añadido).
[277] LO 6/1985, de 1 de julio (BOE N° 157, de 2.7.1985).
[278] Cfr. VELASCO NÚÑEZ, Eloy (2013) "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", en Diario La Ley, Nº 8183, págs. 12/13.
[279] Cfr. SEITZ, Nicolai (2005): "Transborder search…", cit., pág. 36.

Por otro lado, se postula la admisión de una excepción "de buena fe" a la regla de la invalidez de la búsqueda transfronteriza, que se verificaría en el supuesto en que la autoridad encargada de la persecución asume erróneamente que los datos están ubicados en su territorio, o la ubicación del servidor no está clara o no puede ser identificada con certeza. El argumento a favor de esta excepción es que, de lo contrario, el Estado actuante tendría que renunciar significativamente a sus atribuciones en su propio territorio soberano[280]. En contra, puede señalarse que este criterio se presta a ser abusado por las autoridades estatales, toda vez que dejaría en cabeza de las defensas la acreditación de que se actuó "de mala fe", sin que se precise cuál sería el estándar probatorio requerido para lograrlo.

Por añadidura, otro sector de la doctrina sostiene que incluso en búsquedas transfronterizas realizadas a sabiendas (o con la sospecha) de la ubicación extraterritorial de los datos, se podría acceder y recopilar los datos a efectos de ganar tiempo mientras se requiere el permiso del Estado afectado para utilizarlos en un proceso criminal concreto. Entre estos se encuentra Michael SUSSMANN, quien considera que este mecanismo debe ser autorizado cuando concurran "motivos de urgencia" que exijan su uso ("*exigent circumstances*"), como el riesgo inminente para la vida[281]. Esta postura sería aplicable, por ejemplo, a muchos casos vinculados a la explotación sexual infantil, en los que la victimización de los menores suele estar ocurriendo *en tiempo real* mientras se desarrolla la investigación[282].

El déficit del que adolecen los intentos de solución reseñados precedentemente es que todos ellos intentan sortear el obstáculo que representa el principio de territorialidad para la recolección de evidencia en el ciberespacio, pero sin renunciar a sostener la vigencia del mismo, posiblemente en atención al gran arraigo que aquél presenta en la tradición jurídica de la gran mayoría de las naciones del mundo. En orden a ello, un sector de la doctrina -todavía minoritario, pero en continuo crecimiento- señala que la insistencia en aplicar concepciones legales basadas en el principio de territorialidad a la actividad desarrollada en un espacio "no-geográfico" como el ciberespacio carece de sentido y sólo conduce a la confusión[283].

---

[280] Cfr. SEITZ, Nicolai (2005): "Transborder search…", cit., págs. 40/41. Esta es, en esencia, la posición adoptada por la Corte Federal de Apelaciones del 8° Distrito de los EE.UU. en el precedente *Horton*, analizado *Supra*.

[281] Cfr. SEITZ, Nicolai (2005): "Transborder search…", cit., págs. 41/42. En esta línea podría enrolarse una eventual interpretación del art. 18 de la Ley 27.319 que -como se señaló Supra- permite la actuación en extraña jurisdicción cuando hay riesgo para la vida o integridad física de una víctima.

[282] En esa dirección, KOOPS y GOODWIN mencionan dos casos en los Países Bajos en que el Estado actuó en forma extraterritorial atendiendo a la existencia de motivos de urgencia. En el "Caso Bredolab", las autoridades neerlandesas enviaron un mensaje a todas las computadoras infectadas de un *Botnet*, avisándoles de la presencia del virus. Mientras que en el "Caso Descartes", removieron material de explotación sexual infantil de un servidor oculto que probablemente se encontraba en los EE.UU. Atendiendo a esta última circunstancia, las fuerzas de seguridad neerlandesas habían dado aviso a las autoridades estadounidenses de la inminente operación, pero al encontrarse con una gran cantidad de imágenes de explotación sexual infantil que parecían recientes (indicando que el servidor estaba cerca de la fuente del abuso infantil), se decidieron por removerlas directamente, en lugar de recurrir al mecanismo de rogatoria. Luego notificaron a las autoridades en los EE.UU., que no objetaron la operación (Cfr. KOOPS, Bert-Jaap / GOODWIN, Morag (2014): "Cyberspace, the cloud…", cit., pág. 56. Citas omitidas).

[283] Cfr. GOLDSMITH, Jack L. (1999): "Against cyberanarchy", *University of Chicago Law School Occasional Papers*, N° 40, pág. 1 (notas omitidas).

Esta nueva escuela de pensamiento concibe al ciberespacio como un espacio separado, que funciona de un modo diferente al del espacio material y debe ser tratado en consecuencia[284]. Esta postura fue elegantemente sintetizada por John Perry BARLOW –fundador de la Electronic Frontier Foundation- en su hoy célebre "Declaración de Independencia del Ciberespacio", del 8 de febrero de 1996[285], en la que aseveró que los estados "…*no tienen soberanía donde nos juntamos*"[286] (en referencia a los "ciudadanos" del ciberespacio). En esa línea, JOHNSON y POST afirman que las comunicaciones informáticas globales han creado un nuevo "reino" ("*realm*") o ámbito para la actividad humana, que socava la eficacia y legitimidad de las leyes basadas en los límites geográficos. Postulan que existe una nueva frontera, conformada por las pantallas y contraseñas que separan al mundo "real" del "virtual", más allá de la cual se encuentra el ciberespacio, que requiere y puede crear sus propias leyes e instituciones legales. Según los autores, en este ámbito han de surgir nuevas reglas –desvinculadas de las doctrinas atadas a las jurisdicciones territoriales- para gobernar fenómenos novedosos, sin paralelos en el mundo no virtual[287].

Si se enfrenta la problemática en análisis desde la óptica del sector que postula la "independencia" del ciberespacio (mucho más ajustada a la realidad en punto al modo en que se produce el intercambio de información en dicho ámbito), bien podría sostenerse que las autoridades estatales encargadas de investigar delitos que hayan dejado un rastro de evidencia en el ciberespacio están facultadas para acceder a la información digital en las mismas condiciones que cualquier otro "ciudadano" de ese territorio virtual, sin atarse a los límites impuestos por las fronteras territoriales.

Resulta inocultable, sin embargo, que admitir, sin más, que los países están facultados para regular en su derecho interno la posibilidad de acceder remotamente a sistemas ubicados en extraña jurisdicción para obtener evidencia digital –sin autorización expresa del país en que se encuentran los datos- importa renunciar, de una vez y para siempre, a la soberanía que todos ellos afirman ostentar sobre la porción que les toca del ciberespacio. Soberanía que, aunque ilusoria en la práctica, reviste enorme importancia desde el punto de vista jurídico. En esa dirección, vale tener presente que cuando un país afirma que el acceso informático extraterritorial es válido si se cumplen ciertas condiciones establecidas *en su Derecho interno*, ello importa necesariamente aceptar el ejercicio de la misma facultad por parte de *otros* Estados, toda vez que la aceptación recíproca es un principio básico del Derecho internacional[288]. El problema entonces es que, si la medida puede fundarse exclusivamente en normas de derecho interno del país que lleva a cabo el registro transfronterizo, se torna más difícil para el que lo tolera distinguir entre una búsqueda de buena fe en el marco de una investigación penal y una simple excusa para un ciberataque[289].

[284] Cfr. KOOPS, Bert-Jaap / GOODWIN, Morag (2014): "Cyberspace, the cloud…", cit., pág. 31 (citas omitidas).
[285] Disponible en: https://www.eff.org/es/cyberspace-independence.
[286] "You have no sovereignty where we gather".
[287] Cfr. JOHNSON, David R. / POST, David (1996): "Law and borders – The rise of law in cyberspace", en *Stanford Law Review*, Vol. 48, N° 5, pág. 1367.
[288] Cfr. HENNESSEY, Susan (2017): "The elephant in the room…", cit., págs. 31/32.
[289] Los agentes de inteligencia de cualquier Estado podrían, por ejemplo, alegar estar facultados a acceder subrepticiamente a los sistemas informáticos de otros países, con sustento en que ello está justificado por la existencia de una investigación conforme su propia legislación.

Cualquiera sea el enfoque que se adopte, resulta evidente que las consecuencias políticas y diplomáticas pueden tener un alcance global. Por ende, entiendo que asiste razón a DASKAL cuando apunta que las decisiones en orden a esta cuestión deben ser adoptadas por el ala política del gobierno (legisladores y poder ejecutivo) antes que por los jueces[290].

12. Bibliografía

ABEL, Wiebke / SCHAFER, Burkhard (2009): "The German Constitutional Court on the right in confidentiality and integrity of information technology systems – a case report on BVerfG, NJW 2008, 822", en *Scripted*, Vol. 6, N° 1, págs. 106/123.

ANDREWS, Lori / HOLLOWAY, Michael / MASSOGLIA, Dan (2015): "Digital peepholes. Remote activation of webcams: Technology, law, and policy", *Institute for Science, Law and Technology*, ITT Chicago-Kent College of Law.

ASENCIO MELLADO, José María: "La intervención de las comunicaciones y la prueba ilícita", en *Gaceta Penal y Procesal Penal*, Tomo 23, 2011, págs. 155/199.

ATWOOD, J. Riley (2015): "The encryption problem: Why the courts and technology are creating a mess for law enforcement", en *Saint Louis University Law Review*, Vol. 34, págs. 407/433.

AUCOIN, Kaleigh E. (2018): "The spider's parlour: Government malware on the dark web", en *Hastings Law Journal*, Vol 69, N° 5, págs. 1433/1469.

AZFAR, Abdullah / CHOO, Kim-Kwang Raymond / LIU, Lin (2014): "A study of ten popular Android mobile VoIP applications: Are the communications encrypted?", en *47th Annual Hawaii International Conference on System Sciences* (HICSS 2014), IEEE Computer Society Press.

BACHMAIER WINTER, Lorena (2017): "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *Boletín del Ministerio de Justicia*, Madrid, Año LXXI, N° 2195.

BELLOVIN, Steven / BLAZE, Matt / BRICKELL, Ernest / BROOKS, Clinton / CERF, Victor / DIFFIE, Whitfield / LANDAU, Susan / PETERSON, Jon / TREICHLER, John (2006): "Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP", *International Trial Attorneys Association (ITAA)*, publicado el 13/6/2006.

BELLOVIN, Steven M. / BLAZE, Matt / CLARK, Sandy / LANDAU, Susan (2013): "Going bright: Wiretapping without weakening communications infrastructure", en *IEEE Security & Privacy*, Vol 11, N° 1, págs. 62/72.

(2014): "Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet", en *Northwestern Journal of Technology and Intellectual Property*, Vol. 12, N° 1, págs. 1/64.

[290] Cfr. DASKAL, Jennifer (2015); "The un-territoriality of data" cit., pág. 397.

BELLOVIN, Steven M. / BLAZE, Matt / LANDAU, Susan (2016): "Insecure surveillance: Technical issues with remote computer searches", en *Computer – IEEE Computer Society*, págs. 14/24.

BLANCO, Hernán (2020), *Tecnología informática e investigación criminal*, La Ley, Buenos Aires.

BOJARSKI, Kamil (2015): "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations", en *The European Review of Organized Crime*, Vol. 2, N° 2, págs. 25/50.

BRENNER, Susan W. (2012): "Law, dissonance, and remote computer searches", en *North Carolina Journal of Law & Technology*, Vol. 14, N° 1, págs. 43/92.

BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el Fortalecimiento de las Garantías Procesales y la Regulación de las Medidas de Investigación Tecnológica", en *Diario La Ley*, N° 8627, Sección Doctrina, 19/10/2015 (citado de documento electrónico obtenido en: https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAAEAMtMSbF1CTEAAiMjcyMLY7Wy1KLizPw827DM9NS8klQAv991cyAAAAA=WKE).

CARRELL, Nathan E. (2002): "Spying on the mob: United States v. Scarfo – A constitutional analysis", en *Journal of Law, Technology & Policy*", Vol. 2002, N° 1, págs. 193/214.

CASANOVA MARTÍ, Roser (2016): "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", en *Diario La Ley*, N° 8674 (citado de documento electrónico obtenido en https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAAEAMtMSbF1CTEAAiMjS0MLc7Wy1KLizPw827DM9NS8klQAvjXTuiAAAAA=WKE).

CHESNEY, Bobby / CITRON, Danielle (2019): "Deep fakes: A looming challenge for privacy, democracy, and national security", en *California Law Review*, Vol. 107 (citado de documento informático obtenido en: https://scholarship.law.bu.edu/faculty_scholarship/640/).

CLARKE, Zuley / CLAWSON, James / CORDELL, María (2013): "A brief history of hacking", en *Historical approaches to digital media*, Georgia Tech University, LMC 6316.

Consejo de la Unión Europea: "Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime", en *2987th Justice and Home Affairs Council meeting*, 27-28 de noviembre de 2008.

COX, Joseph (2020): "How police secretly took over a global pone network for organized crime", en *Motherboard - Tech by VICE*, publicado el 2/7/2020, obtenido en: https://www.vice.com/en_us/article/3aza95/how-police-took-over-encrochat-hacked.

CUSHING, Tim (2015): "Judge John Facciola on today's law enforcement: I'd go weeks without seeing a warrant for anything 'tactile'", en *TECHDIRT*, publicado el 3/3/2015.

DAHLMANN, Anja (2016): "E-evidence and cross border data requests in Germany", en DE ZAN, Tommaso / AUTOLITANO, Simona (editores), *EUnited against crime: Improving criminal justice in European Union cyberspace,* Instituti Affari Internazionali, págs. 28/41.

DASKAL, Jennifer (2015); "The un-territoriality of data", en *The Yale Law Journal*, Vol. 125, N° 2, págs. 326/398.

Der Spiegel: "Electronic surveillance scandal hits Germany", publicado el 10/10/2011, obtenido en: http://www.spiegel.de/international/germany/the-world-from-berlin-electronic-surveillance-scandal-hits-germany-a-790944.html.

DE ZAN, Tomasso (2016): "E-evidence and cross border data requests in Italy", en DE ZAN, Tommaso / AUTOLITANO, Simona (editores), *EUnited against crime: Improving criminal justice in European Union cyberspace,* Instituti Affari Internazionali, págs. 42/59.

El País: "El móvil del Presidente del Parlament fue objetivo de un programa espía que sólo pueden comprar los gobiernos", publicado el 13/7/2020, obtenido en: https://elpais.com/espana/2020-07-13/el-movil-del-presidente-del-parlament-fue-objetivo-de-un-programa-espia-que-solo-pueden-comprar-gobiernos.html.

Eurojust: "Cybercrime Judicial Monitor", Eurojust Limited, N° 2, noviembre 2016.

Europol (2020): "Dismantling of an encrypted network sends shockwaves through organized crime groups across Europe", publicado el 2/7/2020, obtenido en: https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

Fiscalía General del Estado (2013): Circular 1/2013, de 11 de enero, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

GASSER, Urs / GERTNER, Nancy / GOLDSMITH, Jack / LANDAU, Susan / NYE, Joseph / O'BRIEN, David R. / OLSEN, Matthew G. / RENAN, Daphna / SÁNCHEZ, Julian / SCHNEIER, Bruce / SCHWARTZOL, Larry / ZITTRAIN, Jonathan (2016): "Don't panic. Making progress in the 'going dark' debate", Berkman Center for Internet & Society, Harvard University.

GELLER, Eric (2016): "A complete guide to the new 'Crypto Wars'", en *Daily Dot*, publicado el 26/4/2016 (actualizado el 5/5/2016), obtenido en: http://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/.

GHAPPOUR, Ahmed (2017): "Searching places unknown: Law enforcement jurisdiction on the dark web", en *Stanford Law Review*, Vol. 69, N° 4, págs. 1075/1136.

GOLDE, Nico / REDON, Kevin / BORGAONKAR, Ravishankar (2012): "Weaponizing femtocells: The effect of rogue devices on mobile telecommunication", en *Network and Distributed System Security Symposium* (NDSS), publicado el 6/2/2012, documento informático obtenido en: https://www.tu-berlin.de/fileadmin/fg214/Papers/femto_ndss12.pdf.

GOLDSMITH, Jack L. (1999): "Against cyberanarchy", *University of Chicago Law School Occasional Papers*, N° 40.

GREENBERG, Andy (2014): "Whatsapp just switched on end-to-end encryption for hundreds of millions of users" en *Wired*, publicado el 18/11/2014, obtenido en: http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

GUTHRIE FERGUSON, Andrew (2016): "The Internet of Things and the fourth amendment of effects", en *California Law Review*, Vol. 104, N° 4, págs. 805/880.

HAMMEL SCHULTZ, David (2001): "Unrestricted federal agent: Carnivore and the need to revise the Pen Register Statute", en *Notre Dame Law Review*, Vol. 76, N° 4, págs. 1215/1260.

HASSEMER, Winfried (2000), ¿Proceso penal sin protección de datos?, La insostenible situación del derecho penal, Ed. Comares, Granada.

HENNESSEY, Susan (2017): "The elephant in the room: Addressing child exploitation and going dark", *Aegis Paper Series*, Hoover Institution, Stanford University, N° 1701.

HERN, Alex (2017): "The dilemma of the dark web: Protecting neo-nazis and dissidents alike", en *The Guardian*, publicado el 23/8/2017, obtenido en: https://www.theguardian.com/technology/2017/aug/23/dark-web-neo-nazis-tor-dissidents-white-supremacists-criminals-paedophile-rings.

ISENSEE, Josef (2014), *El derecho constitucional a la seguridad. Sobre los deberes de protección del Estado constitucional liberal*, Rubinzal-Culzoni, Santa Fe.

GIMENO SENDRA, Vicente (2011): "La intervención de las comunicaciones telefónicas y electrónicas", en *Revista 39, Tribuna de Actualidad*, citado de documento electrónico obtenido en http://www.elnotario.es/index.php/hemeroteca/revista-39/697-la-intervencion-de-las-comunicaciones-telefonicas-y-electronicas-0-2863723191305737.

JOHNSON, David R. / POST, David (1996): "Law and borders – The rise of law in cyberspace", en *Stanford Law Review*, Vol. 48, N° 5, págs. 1367/1402.

JOHNSON, M. Eric / MCGUIRE, Dan / WILLEY, Nicholas D. (2008): "The evolution of the peer-to-peer file sharing industry and the security risk for users", en *41 st. Hawaii International Conference on System Sciences, Institute of Electrical and Electronic Engineers (IEEE)*, documento informático obtenido en: https://pdfs.semanticscholar.org/3fa2/84afe4d429c0805d95a4bd9564a7be0c8de3.pdf.

JOYCE, Frederick M. / BIGART, Andrew E. (2007): "Liability for all, privacy for none: The conundrum of protecting privacy rights in a pervasively electronic world", en *Valparaiso University Law Review*, Vol. 41, N° 4, págs. 1841/1516.

KAMINSKI, Liz (2018): "Calling a truce to the Crypto Wars: Why Congress and tech companies must work together to introduce new solutions and legislation to regulate encryption", en *Seton Hall Law Review,* Vol. 48, N° 2, págs. 518/519.

KERR, Orin (2003): "Internet surveillance law after the USA Patriot Act: The big brother that isn't", en *Northwestern University Law Review*, Vol. 97; N° 2, págs. 607/674.

(2004): "The Fourth Amendment and new technologies: Constitutional myths and the case for caution", en *Michigan Law Review*, Vol 102, N° 5 págs. 801/888.

(2005): "Digital evidence and the new criminal procedure", en *Columbia Law Review*, Vol. 105, N° 1, págs. 299/306.

(2005) "Congress, the courts, and new technologies: A response to Professor Solove", en *Fordham Law Review*, Vol. 72, N° 2, págs. 779/790.

KERR, Orin S. / MURPHY, Sean D. (2017): "Government hacking to light the dark web. What risks to international relations and international law?", en *Stanford Law Review Online*, Vol. 70, págs. 58/69.

KOOPS, Bert-Jaap / GOODWIN, Morag (2014): "Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law", *Tilburg Law School Legal Studies Research Paper* Series N° 5/2016.

KOOPS, Bert-Jaap / BEKKERS, Rudi (2017): "Interceptability of telecommunications: Is US and Dutch law prepared for the future?", en *Telecommunications Policy*, Vol. 31, págs. 45/67.

MAYER, Jonathan (2016): "Constitutional malware", en *Social Sciences Research Network* (SSRN), publicado el 14/11/2016.

MITNICK, Kevin D. / SIMON, William L. (2002), *The art of deception. Controlling the human element of security*, John Wiley & Sons, New Jersey.

MONTIERI, Antonio / ACETO, Giuseppe / CIUONZO, Domenico / PESCAPÉ, Antonio (2018): "Anonymity services TOR, I2P, JonDonym: Classifying in the Dark (web)", en *IEEE Transactions on Dependable and Secure Computing*, obtenido en: https://www.researchgate.net/publication/322978661_Anonymity_Services_Tor_I2P_JonDonym_Classifying_in_the_Dark_Web.

MURPHY, Angela (2002): "Cracking the code to privacy: How far can the FBI go?", en *Duke Law & Technology Review,* Vol. 1, págs. 1/6.

NAKASHIMA, Ellen (2015): "Meet the woman in charge of the FBI's most controversial high-tech tools", en *The Washington Post*, publicado el 8/12/2015.

NOSSITER, Adam (2020): "When police are hackers: Hundreds charged as encrypted network is broken", en *The New York Times*, publicado el 2/7/2020, obtenido en: https://www.nytimes.com/2020/07/02/world/europe/encrypted-network-arrests-europe.html.

NUÑEZ, Michael (2017): "FBI drops all charges in child porn case to keep sketchy spying methods secret" en *Gizmodo*, publicado el 7/3/2017, obtenido en: https://www.gizmodo.com.au/2017/03/fbi-drops-all-charges-in-child-porn-case-to-keep-sketchy-spying-methods-secret/.

La Vanguardia: "Pegasus: el móvil de Torrent fue espiado por un programa que solo se vende a gobiernos", publicado el 14/7/2020, obtenido en: https://www.lavanguardia.com/politica/20200714/482313919404/telefono-movil-roger-torrent-president-parlament-programa-espia.html.

LERNER, Zach (2017): "A warrant to hack: An analysis of the proposed amendments to rule 41 of the Federal Rules of Criminal Procedure", en *Yale Journal of Law and Technology*, Vol. 18, N° 1, págs. 26/69.

LÓPEZ-BARAJAS PEREA, Inmaculada (2017): "Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos", en *Revista de Internet, Derecho y Política*, N° 24, págs. 64/75.

O'FLOINN, Micheál (2013): "It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe", en *Computer Law & Security Review*, Vol. 29, págs. 610/615.

ORTIZ PRADILLO, Juan Carlos (2009): "El 'remote forensic software' como herramienta de investigación contra el terrorismo", en *ENAC, E-Newsletter en la lucha contra el cibercrimen*, Cibex, N° 4, págs. 1/9.

(2015): "Fraude y anonimato en la red: Cuestiones constitucionales y procesales de la desanonimización de la red TOR", en SANCHÍS CRESPO, Carolina (directora), *Fraude electrónico. Su gestión penal y civil,* Tirant lo Blanch, Valencia, págs. 55/99.

OWSLEY, Brian L. (2015): "Beware of government agents bearing trojan horses", en *Akron Law Journal*, Vol. 48, N° 2, págs. 315/347.

PELL, Stephanie K / SOGHOIAN, Christopher (2014): "Your secret Stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy", en *Harvard Journal of Law and Technology*, Vol. 28, N° 1, págs. 1/75.

PELROTH, Nicole (2016): "Software as weaponry in a computer-connected world", en *The New York Times*, publicado el 7/6/2016, obtenido en: http://www.nytimes.com/2016/06/09/technology/software-as-weaponry-in-a-computer-connected-world.html?

PÉREZ ESTRADA, Miren Josuné (2019): "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información", en *Revista Brasileira de Direito Processual Penal*, Porto Alegre, Vol. 5, N° 3, págs. 1297/1330.

RON ROMERO, José (2011): "Derecho al secreto de las comunicaciones telefónicas. Un reto para la buena administración" en *Anuario de la Facultad de Derecho de la Universidad de La Coruña*, N° 15/2011, págs. 103/128.

ROXIN, Claus (1997), Derecho Penal. Parte General. Tomo I. Fundamentos. La estructura de la teoría del delito, Civitas, Madrid.

RUBIO ALAMILLO, Javier (2015): "La informática en la reforma de la Ley de Enjuiciamiento Criminal", en *Diario La Ley*, Nº 8663 (citado de documento electrónico obtenido en: https://peritoinformaticocolegiado.es/blog/la-informatica-en-la-reforma-de-la-ley-de-enjuiciamiento-criminal/).

RUIZ LEGAZPI, Ana (2014): "Derecho a la intimidad y obtención de pruebas: el registro de ordenadores (incoming de Emule) en la STC 173/2011", en *Revista Española de Derecho Constitucional*, N° 100, págs. 365/390.

SALT, Marcos (2017), Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos, Ad-Hoc, Buenos Aires.

SATHYAMOORTHY, Dinesh / JALIS, Mohd / SHAFII, Shalini (2014): "Wireless spy devices: A review of technologies and detection methods", en *Defense, Science and Technology Technical Bulletin*, págs. 130/139.

SCHNEIER, Bruce (2006): "Remotely eavesdropping on cell phones microphones", en *Schneier on Security*, publicado el 5/12/2006.

SCHWARTZ, Oscar (2018): "You thought fake news were bad? Deep fakes are were the truth goes to die", en *The Guardian*, publicado el 12/11/2018, obtenido en: https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth.

SEITZ, Nicolai (2005): "Transborder search: A new perspective in law enforcement?", en *Yale Journal of Law and Technology*, Vol. 7, N° 1, págs. 23/50.

SILVA RAMALHO, David (2014): "The use of malware as a means of obtaining evidence in Portuguese criminal proceedings", en *Digital Evidence and Electronic Signature Law Review*, Vol. 11, págs. 55/75.

SKLANSKY, David Alan (2015): "Two more ways not to think about privacy and the Fourth Amendment", en *University of Chicago Law Review*, Vol. 82, N° 1, págs. 223/242.

SPOENLE, Jan (2010): "Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal", *Council of Europe Discussion Paper* N° 31.

SOLOVE, Daniel J. (2005): "Fourth Amendment codification and Professor Kerr's misguided call for judicial deference", en *Fordham Law Review*, Vol. 74, N° 2, págs. 747/777.

SWIRE, Peter / AHMAD, Kenesa (2011): "'Going dark' versus a 'golden age for surveillance'", CDT Fellows Focus Series, publicado el 28/11/2011.

The Guardian: "Dutch arrests after discovery of 'torture chamber' in sea containers", publicado el 7/7/2020, obtenido en: https://www.theguardian.com/world/2020/jul/07/dutch-police-arrest-six-men-after-discovery-of-torture-chamber.

TIMBERG, Craig / NAKASHIMA, Ellen (2013): "FBI's search for 'Mo', suspect in bomb threats, highlights use of malware for surveillance", en *The Washington Post*, publicado el 6/12/2013, obtenido en: https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html.

United Nations Office for Drugs and Crime -UNODC- (2013), *Comprehensive study on cybercrime*, United Nations, Nueva York.

VACIAGO, Giuseppe (2001): "Remote forensics and cloud computing: An Italian and European legal overview", en *Digital Evidence and Electronic Signature Law Review*, Vol. 8, págs. 124/129.

VEGAS TORRES, Jaime (2017); "Las medidas de investigación tecnológica", en CEDEÑO HERNÁN, M. (coord.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Navarra, págs. 21/47 (Citado de documento informático obtenido en: https://zenodo.org/record/1042742#.Xx8aW55KjIU).

VELASCO NÚÑEZ, Eloy (2007): "Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos)", en *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia,* Cuadernos de Derecho Judicial, 2007-II, CGPJ, págs. 77/124.

(2011): "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías" en *Revista de Jurisprudencia*, N° 4, citado de documento electrónico obtenido en: https://elderecho.com/novedades-tecnicas-de-investigacion-penal-vinculadas-a-las-nuevas-tecnologias.

(2013) "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", en *Diario La Ley*, Nº 8183, págs. 1/24.

WALDEN, Ian (2011): "Accessing data in the cloud: The long arm of the law enforcement agent", en *Queen Mary School of Law Legal Studies*, Research Paper N° 74/2011.

WikiLeaks: "Press release: Vault 7", publicada el 7/3/2017.