FEDERICA CENTORAME[*]

INVESTIGACIONES CRIMINALES INTRUSIVAS Y BÚSQUEDA DE PRUEBAS A TRAVÉS DE "*SOFTWARE* ESPÍAS" EN LA EXPERIENCIA PROCESAL ITALIANA[**]

RESUMO. *Este artículo se ocupa de examinar el uso que la práctica italiana hace de los programas informáticos de espionaje como medio atípico de investigación criminal, al margen de un marco normativo de referencia. Con las evidentes consecuencias que se derivan para la protección equitativa de los derechos fundamentales afectados por la captura tecnológica.*

[*] Investigadora en Derecho procesal penal, Departamento de Derecho, Universidad de Roma Tre.

[**] Texto reelaborado y ampliado de la ponencia presentada en el marco de la *I Jornada Internacional De Jóvenes Investigadores* (21 y 22 de abril 2021), organizada por la Universitat de Girona sobre el tema "*Investigación y proceso penal en el siglo XXI. Nuevas tecnologías y protección de datos*".

1. Algunas consideraciones de fondo

En la experiencia italiana, el uso de programas informáticos de espionaje como instrumentos de búsqueda de pruebas ofrece una muestra muy representativa de la radical metamorfosis que ha sufrido la investigación criminal debido al continuo progreso de la tecnología.

Incluso los no profesionales están ahora familiarizados con el funcionamiento de este dispositivo. Se trata de un *malware* capaz de controlar de forma remota el dispositivo electrónico en el que está instalado, mediante el acceso manual al propio dispositivo así como, más frecuentemente, mediante una inoculación sigilosa a través de Internet, simplemente enviando un correo electrónico o durante una operación de actualización[1].

Introducido en el soporte informático de destino, el programa espía es capaz de vigilar toda la actividad realizada a través del mismo dispositivo y de operar como si tuviera la disponibilidad física, sin detectar nunca su propia presencia interna[2].

De esta manera, los investigadores pueden buscar, vigilar y adquirir de forma encubierta cualquier contenido informativo introducido en la red por usuarios individuales, en diversas capacidades implicados en el caso[3].

La información digital, contenida en los dispositivos electrónicos, constituye, de hecho, un instrumento ineliminable en la fase de investigación[4], tanto para documentar la comisión ocasional de delitos comunes a través del instrumento informático, como para averiguar casos más específicos, como los de carácter terrorista, cuya comprobación puede hacerse en tiempo real a través de la vigilancia electrónica de la con-

[1] Para un análisis de la capacidad de intrusión del virus espía, véase R. Brighi, *Requisiti tecnici, potenzialità e limiti del captatore informatico. Analisi sul piano informatico-forense*, en G. Giostra-R. Orlandi (editado por), *Revisioni normative in tema di intercettazioni. Riservatezza, garanzie difensive e nuove tecnologie informatiche*, Giappichelli, Torino, 2021, pp. 231 ss.

[2] Al respecto, A. Sanna, *L'irriducibile atipicità delle intercettazioni tramite* virus *informatico*, en A. Scalfati (a cargo de), *Le indagini atipiche*, II ed., Giappichelli, Torino, 2019, p. 604.

[3] Así, C. Conti, *Sicurezza e riservatezza*, en *Diritto penale e processo,* 2019, p. 1574.

[4] Desde un punto de vista monográfico, sobre el tema, consúltense los recientes trabajos de M. Pittiruti, Digital Evidence *e procedimento penale,* Giappichelli, Torino, 2017; S. Signorato, *Le indagini digitali: profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018.

ducta proselitista vía *web*[5].

Todo esto es suficiente para encontrar las razones más profundas del recurso cada vez mayor a los dispositivos tecnológicos para la búsqueda de pruebas.

Además de la necesidad de oponerse, con medios adecuados al efecto, a la evolución ontológica de las formas delictivas, determinada precisamente por el uso masivo de los sistemas digitales[6], la creciente utilización, con fines de investigación, de sofisticadas tecnologías de vigilancia secreta y constante de las personas se explica a la luz de los efectos perturbadores que estas herramientas son capaces de provocar sobre las mismas coordenadas teóricas en las que hasta ahora se ha enmarcado el tema de la verdad en el proceso penal.

Aplicados en el terreno probatorio, los citados medios de vigilancia electrónica permiten al Juez no sólo reconstruir, con precisión, el hecho pasado sometido a su escrutinio, sino incluso asistir a la repetición fiel del hecho que debe ser juzgado[7].

De este modo, pasamos de una verificación veraz, pero todavía aproximada, ya que está condicionada por los insuperables límites cognitivos de la narración testimonial a la que tradicionalmente se confía la reevocación del episodio criminal, al realismo gnoseológico de la "verdad digital"[8], que, aunque diferida, es capaz de representar fielmente la misma conducta objeto del juicio.

Sin embargo, es necesario preguntarse inmediatamente hasta dónde estaríamos dispuestos a llegar para obtener la aportación probatoria de ese conocimiento (aparen-

[5] Véase G. Paolozzi, *Relazione introduttiva*, en L. Lupária-L. Marafioti-G. Paolozzi (a cargo de), *Dimensione tecnologica e prova penale*, Giappichelli, Torino, 2019, p. 9; en concreto, sobre la conexión entre las herramientas de investigación intrusiva y la lucha contra el terrorismo, véase M. Daniele, *Contrasto al terrorismo e captatori informatici*», en *Rivista di diritto processuale*, 2017, pp. 393 ss.

[6] Sobre este punto, véase L. Lupária, Computer crime *e procedimento penale*, en G. Garuti (editado por), *Modelli differenziati di accertamento*, en *Trattato di procedura penale*, dirigido por G. Spangher, Utet, Torino, 2011, p. 369; M. Torre, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, en *Diritto penale e processo,* 2015, p. 1163.

[7] En este sentido, O. Mazza, *La verità giudiziale nel sistema delle prove tecnologiche*, in Id., *Tradimenti di un codice. La Procedura penale a trent'anni dalla grande riforma*, Giappichelli, Torino, 2020, p. 8.

[8] La expresión es de F. Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, en Lupária-Marafioti-Paolozzi (a cargo de), *Dimensione tecnologica e prova penale*, cit., p. 45

temente) "perfecto"[9] en cuanto al resultado de la comprobación del hecho del delito en el juicio.

La indiscutible utilidad heurística de la información que puede adquirirse mediante instrumentos tecnológicos siempre más sofisticados y intrusivos, centrando la atención en el único resultado cognitivo del hecho que se constata, tiende a perder el sentido constitucional del proceso penal como sistema de límites en el que se encauza el poder de castigar[10].

Así, se corre el riesgo de llegar al peligroso malentendido de que, en el procedimiento de reconstrucción de los hechos controvertidos, las formas procesales y las limitaciones probatorias no son más que un instrumento técnico, como tal, neutral e independiente respecto a los valores[11]. Y de ello se deriva otra paradoja: las actividades de investigación, justificadas por la represión de delitos agresivos contra los bienes jurídicos de los ciudadanos, pueden acabar comprimiendo los derechos y libertades fundamentales de las personas, a través de una injerencia incontrolada de la autoridad en la existencia privada de cada individuo[12].

2. Cuestiones no resueltas en la regulación jurídica de las intervenciones de comunicaciones mediante virus informáticos

Muy consciente de estos escollos para las prerrogativas de los particulares, el legislador italiano ha puesto recientemente la atención en una funcionalidad técnica específica del *software* espía. Es decir, la activación a distancia del micrófono o la cámara *web* integrados en el dispositivo.

De esta manera, es posible realizar una aprehensión oculta y continua de las

[9] Con énfasis crítico, habla de "prova perfetta" con referencia a la prueba digital, L. Marafioti, Digital evidence *e processo penale*, en *Cassazione penale,* 2011, p. 4510.

[10] En un sentido compartido, F. Cordero, *Procedura penale*, Giuffrè, Milano, 1983, p. 584.

[11] El argumento está tomado, por el contrario, de G. De Luca, *La cultura della prova e il nuovo processo penale*, en Aa.Vv*., Evoluzione e riforma del diritto e della procedura penale. Scritti in onore di G. Vassalli*, vol. II, Giuffrè, Milano, 1991, p. 184. Sobre el tema de las formas procesales como valores ético-políticos, véase M. Nobili, *Forme e valori*, (1993), ahora en Id., *Scenari e trasformazioni del processo penale*, Cedam, Padova, 1998, pp. 1 ss.

[12] F. Nicolicchia, *Il controllo occulto e continuativo come categoria probatoria: premesse teoriche di una sistematizzazione*, en *Diritto penale contemporaneo – Rivista trimestrale,* 2019, 2, p. 431.

conversaciones y de los comportamientos comunicativos entretenidos por la persona que tiene la disponibilidad material del dispositivo y por todos aquellos que se encuentran dentro del rango operativo del dispositivo infectado[13].

A pesar de un uso descuido del instrumento examinado, ya largamente establecido en la práctica de las Fiscalías[14], el reconocimiento normativo formal de la técnica de investigación basada en programas de espionaje se debe, en Italia, por primera vez, al Decreto Legislativo de 29 de diciembre de 2017, n. 216, cuya disciplina sobre el punto, retocada por el Decreto Legislativo de 31 de diciembre de 2019, n. 161, ha entrado en pleno funcionamiento, tras múltiples prórrogas, el pasado 1 de septiembre de 2020 .

En particular, las citadas medidas legislativas, al modificar los artículos 266 y siguientes del Código procesal penal, han previsto expresamente que la actividad de intervención de las comunicaciones entre las personas presentes "también puede realizarse mediante la inserción de un virus informático en un dispositivo electrónico portátil". Y esto también se permite en el domicilio, siempre que – tratándose de delitos comunes – existan indicios serios de que en los lugares reservados se está realizando una "actividad delictiva".

Hay que decir que esta iniciativa del Legislador intervino en rápida sucesión cronológica con respecto a un importante pronunciamiento de las Secciones Unidas del Tribunal Supremo italiano[15].

Los jueces de la legitimidad, abordando la cuestión relativa al uso probatorio de la intervención encubierta de conversaciones a través de virus informáticos, habían, de hecho, circunscrito el campo de aplicación sólo a los delitos de delincuencia organizada, para los que la disciplina tradicional de las interceptaciones admite la actividad de captación también en lugares de residencia privada, sin necesidad de un "motivo fun-

[13] Entre otros, véase, D. Curtotti, *Il captatore informatico nella legislazione italiana*, en *Jus*, 2017, 3, pp. 382 ss.; M. Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, Milano, 2017, pp. 12 ss.

[14] Prueba de ello es que el Tribunal Supremo lleva tratando el tema desde 2009: Cass., Sec. V, 14 de octubre de 2009, núm. 16556, (CED, rv. 246954).

[15] Cass., Sect. Un., 28 de abril de 2016, núm. 26889, en *Archivio della nuova procedura penale*, 2017, pp. 76 ss.

dado para creer que allí se está realizando la actividad delictiva".

Por lo tanto, la utilización de medios de investigación encubiertos debía considerarse prohibida para todo el ámbito de los procedimientos relativos a los delitos comunes.

En estos casos – según el Tribunal de Casación – el carácter itinerante de la interceptación a distancia mediante programas informáticos de espionaje, que impide conocer de antemano los movimientos del instrumento móvil, supondría, de hecho, siempre el riesgo de que la red de investigadores acabe con comunicaciones que no pueden ser legítimamente interceptadas por tener lugar en un contexto doméstico en el que no se están cometiendo delitos[16].

Sin embargo, el legislador italiano ha ido mucho más allá. No sólo ha extendido el uso incondicional, propio de los supuestos penales asociativos, a la categoría de los delitos de corrupción contra la administración pública[17], sino que, sobre todo, ha considerado compatible el carácter fisiológicamente itinerante de los medios intrusivos con la protección reforzada, ya prevista por el Código procesal para las intervenciones ambientales dentro de los lugares domiciliarios[18]. Y ha reafirmado, así, la operatividad investigadora del *software* espia en los ámbitos de la vivienda privada, también en relación con todos los delitos comunes para los que se admite la intervención ordinaria, siempre que subsista el ulterior requisito de gravedad circunstancial respecto a la realización efectiva de la actividad delictiva en los mismos lugares reservados.

Para este fin, según el Legislador, es suficiente que la medida con la que el juez de instrucción autorice la intrusión informática indique "los lugares y el tiempo, también determinados indirectamente, en relación con los cuales se permite la activación del micrófono". Y la garantía de la inviolabilidad del domicilio se deja, en cambio, al operador individual, que tiene la tarea de identificar los lugares de residencia privada que deben

[16] F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, en *Revista brasileira de direito procesal penal,* 2017, vol. 3, 2, p. 497.

[17] A este respecto, véase A. Procaccino-W. Nocerino, *Le nuove investigazioni nei reati corruttivi informatici*, en *Diritto penale e processo,* 2020, p. 1626.

[18] M. Torre, *Il captatore informatico, tra riforma Orlando e sistema processuale*, en *Giurisprudenza italiana,* 2018, p. 1777.

ser retirados de la actividad de captación, ajustando para ello, el encendido del micrófono en base a lo establecido en el decreto de autorización[19].

A mi juicio, es una solución poco tranquilizadora desde el punto de vista de la eficacia de la protección del núcleo duro de los derechos fundamentales afectados por el uso del virus informático.

Parece claro, en efecto, que la opción legislativa, situando el control del juez en la sola fase de autorización de la intervención informática y no también durante la ejecución de la misma[20], es inadecuada para conjurar el riesgo de un uso anormal de la intervención[21], es decir, desproporcionado respecto a la compresión del derecho a la intimidad del domicilio que, en abstracto, se quiere preservar.

En apoyo del supuesto, basta considerar que el Tribunal Europeo de Derechos Humanos, al perfilar las garantías mínimas que los distintos legisladores nacionales deben ofrecer en materia de interceptación, incluyó precisamente la facultad de revisión *in itinere* por parte del tribunal nacional de las operaciones de captación[22].

Las perplejidades, sin embargo, no se agotan en esta observación.

Otras objeciones contra la capacidad concreta de la disciplina normativa de realizar un correcto equilibrio entre la potencial fuerza invasiva del bug informático y la inevitable lesión de los derechos fundamentales consiguiente, surgen de los expedientes, aunque meritorios, con los que el Legislador italiano pretendió remodelar el acto típico de la interceptación de las comunicaciones para adaptarlo a la captura tecnológica en cuestión[23].

En efecto, es cierto que algunas disposiciones de reciente cuño, destinadas a ga-

[19] Ver, de nuevo, TORRE, *Il captatore informatico, tra riforma Orlando e sistema processuale*, cit., pp. 1777-1778.

[20] S. FURFARO, voce «*Intercettazioni (profili di riforma)*», en *Digesto delle discipline penalistiche,* X, Utet, Torino, 2018, p. 404.

[21] En este sentido, L. AGOSTINO-M. PERALDO, *Le intercettazioni con captatore informatico: ambito di applicazione e garanzie procedurali*, en M. GIALUZ (editado por), *Le nuove intercettazioni*, en *Diritto di internet*, 2020, 3, p. 80.

[22] Tribunal europeo de derechos humanos, 18 de mayo de 2010, *Kennedy* v. Reino Unido; Id., 31 de mayo de 2005, *Vetter* v. Francia; Id., 27 de julio de 2003, *Hewitson* v. Reino Unido.

[23] Sobre este punto, véase C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, en *Diritto penale e processo*, 2018, pp. 1218-1219; DANIELE, *L'illusione di domare il captatore informatico*, en *www.lalegislazionepenale.eu*, 24 de noviembre de 2020, p. 58.

rantizar que el *software* de espionaje utilizado para la recepción encubierta se limite a realizar las operaciones expresamente ordenadas según estándares adecuados de fiabilidad técnica, seguridad y eficacia[24], denotan el compromiso legislativo de oponerse a una adquisición inmoderada de datos[25] que puedan ser atacados por la intrusión informática. Y así tienden a conformar el sistema interno a los principios de cautela y protección de la integridad y autenticidad de la información captada, establecidos por la Directiva 2016/680/UE sobre protección de datos en el ámbito de la cooperación judicial y policial. Directiva que evidentemente también se aplica al caso en cuestión, realizando el uso del *software* espía un tratamiento masivo de datos personales con fines de lucha contra los delitos[26].

Se hace referencia, por ejemplo, a las prescripciones contenidas en el artículo 89, Disposiciones de aplicación del código de derecho procesal penal, en virtud del cual, entre otras cosas, se establece que el informe de las interceptaciones a distancia debe indicar el tipo de *software* utilizado, de conformidad con los requisitos técnicos establecidos con Decreto del Ministerio de Justicia y se prevé la obligación de desactivar el interceptor "con modalidades tales que lo hagan inadecuado para su uso posterior", una vez concluidas las operaciones.

Sin embargo, la cuestión es que estas prescripciones carecen de una sanción formal en el caso de una transgresión relativa[27]. Y en ausencia de sanciones específicas que garanticen su eficacia, cualquier norma procesal se convierte en una simple recomendación, de la que siempre se puede apartar en su aplicación[28].

[24] Torre, *D.M. 20 aprile 2018: le disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico*, en *Diritto penale e processo,* 2018, p. 1256.

[25] Véase, T. Bene, *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, en *Archivio penale web*., 2019, 3, p. 5.

[26] A este respecto, véase S. Signorato, *Rimodulazioni normative dell'uso investigativo del captatore informatico*, en . Giostra-Orlandi (editado por), *Revisioni normative in tema di intercettazioni*, cit., p. 332.

[27] G. Galantini, *Profili di inutilizzabilità delle intercettazioni anche alla luce della nuova disciplina*, en *Diritto penale contemporaneo,* 16 de marzo de 2018, p. 12.

[28] Véase M. Caianiello, *To Sanction (or not to sanction) Procedural Flaws at EU Level? A Step forward in the Creation of an EU Criminal Process,* en *European Journal of Crime, Criminal Law and Criminal Justice*, 2014, p. 319; A. Marandola, *Il modello sanzionatorio tra vecchio e nuovo sistema processuale*, in Ead. (editado por), *Le invalidità processuali. Profili statici e dinamici*, Utet, Torino, 2015, p. 7.

Esto es lo que ha sucedido con respecto a los mencionados cambios normativos en materia de intervencíon mediante trojan virus.

El Legislador italiano no ha actualizado el artículo 271 que, en el Código procesal penal italiano, enumera de manera perentoria las violaciones normativas relativas al caso de interceptación, sancionadas con la inutilización de los resultados relativos[29]. Y tal omisión, lejos de reforzar las barreras protectoras de los derechos fundamentales afectados por la peculiar agresividad del instrumento de captación tecnológica, es equivalente a autorizar el máximo sacrificio, sin siquiera el exiguo consuelo de un remedio tardío, destinado a prohibir el uso probatorio de los contenidos lesivos de tales derechos[30].

3. El programa de espionaje como diligencia de investigación atípica en la práctica de la jurisprudencia

Otra cuestión distinta es que el legislador de la reforma tampoco ha previsto nada sobre las otras formas de vigilancia y control encubiertos que pueden llevarse a cabo mediante el uso del instrumento tecnológico intrusivo[31]. Como, por ejemplo, la capacidad del *software* para conseguir una verdadera búsqueda remota de los archivos del dispositivo infectado, adquiriendo una copia de todo su contenido[32].

De este modo, se deja al intérprete entender si tal comportamiento silencioso equivale o no a excluir el uso investigativo del *software* de espionaje para las demás fun-

[29] La observación es de GALANTINI, *Profili di inutilizzabilità delle intercettazioni anche alla luce della nuova disciplina*, cit. p. 12; en sentido análogo, DANIELE, *L'illusione di domare il captatore informatico*, cit., p. 59, quien habla a este respecto de "*leges minus quam perfectae*".

[30] En un sentido compartido, L. PARLATO, *Le perquisizioni* on-line*: un tema che resta un tabù*, en Giostra-Orlandi (editado por), *Revisioni normative in tema di intercettazioni,* cit., p. 368.

[31] En dicha omisión encuentran una auténtica limitación de la intervención legislativa D. CURTOTTI-W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, in G.M. Baccari- C. Bonzano-K. La Regina-E.M. Mancuso (editado por), *Le recenti riforme in materia penale*, Cedam, Padova, 2018, p. 544.

[32] Sobre el tema, véase, entre otros, CONTI-TORRE, *Spionaggio informatico nell'ambito dei* social network, en Scalfati (editado por), *Le indagini atipiche*, cit., p. 535 ss.; P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, en T. Bene (a cargo de), *L'intercettazione di comunicazioni*, Cacucci, Bari, 2018, p. 303 ss.; E.M. MANCUSO, *La perquisizione* on-line, en *Jus*, 2017, 3, p. 414 ss.; PARLATO, *Problemi insoluti: le perquisizioni* on-line, en Giostra-Orlandi (editado por), *Nuove norme in tema di intercettazioni*, cit., pp. 289 ss.

ciones mencionadas anteriormente.

En este sentido, hay que decir que basándose en la correcta interpretación de las disposiciones del procedimiento penal[33] como límites a la acción de la autoridad procesal sería bastante fácil responder afirmativamente a la cuestión recién formulada[34]. Consecuencia de lo anterior es que todo lo que no está expresamente regulado dentro de las prescripciones normativas vigentes estaría implícitamente prohibido, precisamente por exceder los límites canónicos de la liturgia procesal.

No obstante, la jurisprudencia no se ha pronunciado hasta ahora en el mismo sentido.

El Tribunal de Casación italiano, en particular, ha sostenido que es legítimo registrar a distancia el dispositivo afectado por el virus, llevando a la categoría de prueba atípica a que se refiere el artículo 189 del Código procesal penal (CPP) la obtención -mediante un *software* espia- de la documentación informática memorizada en el ordenador personal en uso por el acusado (...), si la medida se ha referido a la extrapolación de datos, que no tienen por objeto un flujo de comunicaciones, ya formados y contenidos en la memoria del ordenador personal o que habrían sido memorizados en el futuro[35].

Esta suposición merece un poco más de atención.

Muy resumidamente, con dicha disposición el legislador italiano ha previsto la posibilidad de que el juez admita en el juicio pruebas no reguladas por la ley para abrir el proceso penal a nuevas formas de conocimiento, en constante ajuste al desarrollo tecnológico que amplía las fronteras de la investigación[36].

Para ello, el citado artículo 189 CPP exige la observancia de un triple orden de

[33] Así, MAZZA, *Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni*, en ID., *Tradimenti di un codice*, cit., p. 154.

[34] Se sigue aquí el planteamiento de G. ILLUMINATI, *Libertà e segretezza delle comunicazioni*, en *Cassazione penale,* 2019, p. 3830, según el cual debe deducirse, en base al principio de taxatividad, que lo que no está expresamente permitido debe considerarse prohibido.

[35] Cass., Sec. V, 14 de octubre de 2009, núm. 16556 (CED, rv. 246954); en sentido similar, Cass., Sec. V, 30 de mayo de 2017, núm. 48370 (CED, rv. 271412).

[36] Así, *Relazione al Progetto preliminare del 1988*, en G. CONSO-V. GREVI-G. NEPPI MODONA, *Il nuovo codice di procedura. Dalle leggi ai decreti delegati, IV, Il progetto preliminare del 1988*, Cedam, Padova, 1990, p. 533.

condiciones. Debe ser una aportación probatoria "idónea para asegurar la averiguación de los hechos"; es necesario que la asunción relativa no "perjudique la libertad moral de la persona" afectada; es necesario, finalmente, que antes de proceder a la admisión, el Juez "sentencie a las partes sobre la modalidad de asunción de la prueba".

Por lo tanto, es a la luz de cada uno de estos requisitos legales que es necesario examinar los méritos del enfoque jurisprudencial descrito anteriormente, inclinado a permitir el uso investigativo multiforme de la escucha informática, como medio atípico de investigación de la prueba[37].

Ahora bien, si no parece haber dudas sobre la capacidad del instrumento tecnológico en cuestión para aportar una contribución decisiva a la reconstrucción de los hechos investigados[38], parece, en cambio, mucho más problemático sostener su cumplimiento de las otras dos condiciones exigidas por la ley procesal.

Por un lado, es oportuno recordar que la inoculación del *software* de espionaje dentro del dispositivo de destino, que tiene lugar, con frecuencia, con la colaboración inconsciente del destinatario, engañado por un enlace presente en un correo electrónico o por una solicitud de actualización de una aplicación, es capaz de realizar los propios extremos de una violación de la libertad moral de la persona implicada[39].

De hecho, al descargar el virus informático sin saberlo, la persona que tiene acceso al dispositivo infectado acaba realizando una acción potencialmente autoinculpatoria, en clara violación del canon "*nemo tenetur se detegere*"[40]. Principio que, en los

[37] En una opinión coincidente, M. Bontempelli, *Il captatore informatico in attesa della riforma,* en *Diritto penale contemporaneo,* 14 de diciembre de 2018, p. 14.

[38] Véase Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 486; Mazza, *La verità giudiziale nel sistema delle prove tecnologiche,* cit., p. 18; Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 69.

[39] De esta opinión, Bontempelli, *Il captatore informatico in attesa della riforma,* cit., pp. 14-15; R. Brighi, *Funzionamento e potenzialità investigative del* malware*,* cit., p. 219; Signorato, *Le indagini telematiche*, cit., pp. 237-238. Sin embargo, según la jurisprudencia del Tribunal Supremo italiano, el virus informático no ejerce ninguna presión sobre la libertad física y moral de la persona, no pretende manipular ni forzar una aportación declarativa, sino que, dentro de los estrictos límites en que se permiten las interceptaciones, capta las comunicaciones entre terceras personas, en su genuinidad y espontaneidad: Cass., Sec. V, 30 de septiembre de 2020, núm. 31604, en *www.dirittoegiustizia.it*, 12 de noviembre de 2020.

[40] Lo señala, de nuevo, Signorato, *Le indagini telematiche*, cit., p. 237.

sistemas procesales liberales, tiene como objetivo proteger los actos y las palabras del individuo de formas perjudiciales para el derecho a un ofrecimiento voluntario a los órganos de investigación[41].

Por otro lado, parece algo cuestionable que el uso atípico de los medios tecnológicos intrusivos logre satisfacer el estándar necesario de interlocución con las partes del juicio interesadas por el empleo relativo, al que alude el mencionado artículo 189 del Código procesal penal.

En este sentido, basta considerar la posición de clara inferioridad argumental, frente a la contraparte pública, en la que, en tal caso, se ve obligado el abogado del demandado. Este último, al que la jurisprudencia italiana atribuye la carga de probar que, en el caso concreto, la tecnología de investigación utilizada ha comprometido la fiabilidad del elemento cognoscitivo que se haya podido adquirir[42], debería poder tener libre acceso a la información relativa al *software* mediante el cual se tomaron las pruebas y a las técnicas forenses adoptadas para ello por los investigadores[43].

El condicional, sin embargo, es obligatorio, ya que en presencia de pruebas algorítmicas[44], como las que se forman a través del *software* de espionaje, la defensa suele sufrir considerables dificultades en cuanto al conocimiento del código fuente que gobierna el modelo computacional con el que se han elaborado los datos, del que se pretende falsear la exactitud[45].

La razón es que el programa en la base del agente intruso basa su eficacia en el secreto de su funcionamiento; mientras que la posibilidad de conocer las instrucciones del programa permitiría a cualquier persona con un mínimo de conocimientos técnico-

[41] Lupária, Privacy, *diritti della persona e processo penale*, en *Rivista di diritto processuale,* 2019, p. 1465.

[42] Cass., Sec. III, 28 de mayo de 2015, núm. 37644, (CED, rv. 265180); Id., Sec. I, 5 de marzo de 2009, núm. 14511, (CED, rv. 243150).

[43] Sobre este punto, véase F. Palmiotto, *Captatori informatici e diritto alla difesa. Il caso Exodus*, en *www.lalegislazionepenale.eu*, 16 ottobre 2020, p. 19.

[44] Desde un punto de vista monográfico, para todos, remítase al reciente estudio de S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, Springer, 2020.

[45] Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo,* en *Revista Italo-Espanola de Derecho Procesal*, vol. I, 2019, p. 120; al respecto, véase también V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, en *disCrimen*, 15 de mayo de 2020, p. 14.

informáticos tomar las contramedidas adecuadas para burlarlo[46].

Este régimen de secreto se traduce en la imposibilidad, para la defensa, de verificar, *a posteriori*, la salida del algoritmo[47]. Lo cual, no sólo evoca una representación extrema de la posible violación de la igualdad de armas[48] entre las contrapartes del juicio, sino que, sobre todo, comprime la garantía del contrainterrogatorio, entendido también como una verificación póstuma sobre la corrección de la investigación informática[49].

4. La legalidad formal como única protección contra las interferencias tecnológicas en la investigación penal

Pero es en el plano constitucional donde se plantean las cuestiones más críticas.

La Constitución italiana, de hecho, prohíbe el uso de instrumentos atípicos para la búsqueda de pruebas siempre que afecten a derechos individuales definidos como inviolables por la propia Constitución: es decir, la libertad personal, la intimidad del hogar y el secreto de las comunicaciones[50].

En cada uno de estos ámbitos, además de la reserva de competencia al poder jurisdiccional único, la Carta Fundamental exige que sea la ley ordinaria la que establezca con precisión en qué casos, con qué modalidades y con qué garantías se pueden violar

[46] Así lo destaca G. Ziccardi, *Il captatore informatico nella "riforma Orlando": alcune riflessioni informatico-giuridiche*, en *Archivio penale,* 2018, 1, Speciale Riforme, p. 506. A este respecto, véase además Brighi, *Requisiti tecnici, potenzialità e limiti del captatore informatico*, cit., p. 255.

[47] Otra vez, Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della Convenzione europea dei diritti dell'uomo*, cit., p. 120.

[48] De esta opinión, Quattrocolo, *Qualcosa di meglio del diritto (e del processo) penale?,* in *disCrimen*, 26 de junio de 2020, p. 7.

[49] En este sentido, Felicioni, *Le ispezioni e le perquisizioni*, en G. Ubertis-G.P. Voena (dirigido por), *Trattato di procedura penale,* vol. XX, Giuffrè, Milano, 2012, p. 245. Pero la literatura procesal penal sobre el punto es muy amplia: entre otros, véase R. Kostoris, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, en F. Ruggieri-L. Picotti (editado por), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica: aspetti sostanziali e processuali*, Giappichelli, Torino, 2011, p. 181; L. Lupária, *La disciplina processuale e le garanzie difensive*, en Lupária-Ziccardi (editado por), *Investigazione penale e tecnologia informatica,* Giuffrè, Milano, 2007 cit., p. 128; L. Marafioti, Digital evidence *e processo penale*, cit., p. 4509; Pittiruti, Digital Evidence e *procedimento penale*, cit., pp. 161 ss.

[50] En este sentido se manifiesta Caprioli, *Il "captatore informatico" come mezzo di ricerca della prova in Italia*, cit., p. 487; Conti-Torre, *Spionaggio digitale nell'ambito dei* social network, cit., p. 536.

los derechos en cuestión[51].

Las limitaciones en la esfera individual causadas por el uso investigativo de *software* de espionaje ciertamente no escapan al alcance de tal prohibición constitucional.

Los múltiples servicios ofrecidos por el dispositivo de captación, que permiten a los investigadores vigilar a distancia, en secreto y sin límites espacio-temporales, cualquier actividad del sujeto pasivo, representan una amenaza actual para las renovadas instancias de confidencialidad que la modernidad pone en la protección del individuo informatizado[52].

En particular, la vigilancia continua y oculta que proporcionan los programas de espionaje ataca la intimidad de la esfera doméstica informática[53] que, hoy en día, cada uno de nosotros ocupa dentro del universo digital.

Como subraya la doctrina, la actual sociedad cibernética ha delimitado las fronteras de un espacio virtual "doméstico" sin precedentes, dentro del cual los usuarios individuales deben poder manifestar y desarrollar libremente su propia personalidad, protegidos de ojos y oídos indiscretos[54].

Así pues, ha surgido una nueva libertad fundamental, que merece una protección según las normas constitucionales al menos a la par que la inviolabilidad del domicilio físico sancionada por el artículo 14 de la Constitución italiana[55].

De ahí que la conclusión del razonamiento sea obligatoria.

Cualquier injerencia investigadora en el domicilio informático, afectando a un derecho subjetivo inviolable cuya limitación no ha sido regulada aún por la ley proce-

[51] Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 487.

[52] Véase W. Nocerino, *Il captatore informatico: un giano bifronte*. *Prassi operative* vs *risvolti giuridici*, en *Cassazione penale,* 2020, p. 830.

[53] Sobre el domicilio informático como bien fundamental afectado por las intrusiones tecnológicas, véase A. Camon, *Cavalli di Troia in Cassazione,* en *Archivio della nuova procedura penale,* 2017, 1, p. 95; F. Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, cit., p. 49; Parlato, *Problemi insoluti: le perquisizioni* online, en Giostra-Orlandi (editado por), *Nuove norme in tema di intercettazione*, cit., p. 302; Ead., *Le perquisizioni* on-line: *un tema che resta un tabù*, en Giostra-Orlandi (editado por), *Revisioni normative in tema di intercettazioni*, cit., p. 350.

[54] En estos términos, Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, cit., p. 49.

[55] Se sigue la opción de Conti, *Sicurezza e riservatezza,* cit., p. 1575.

sal[56], es constitucionalmente inaceptable[57]. De hecho, vulnera la reserva legislativa que la Constitución italiana establece como límite insuperable para que la autoridad judicial pueda suprimir una libertad fundamental, de acuerdo con el principio de proporcionalidad de los medios al fin[58].

Este principio representa un corolario de la propia inviolabilidad de las prerrogativas individuales puestas en peligro por el ejercicio de los poderes de búsqueda de pruebas en el proceso penal[59]. Opera, en primer lugar, respecto del legislador, obligándole a seleccionar los requisitos procesales idóneos para interferir en la esfera individual y, después, se refleja en el juez llamado a elegir la opción jurídica menos gravosa en el caso concreto[60].

Se trata de un "orden de precedencia" que no es en absoluto casual y que ha de tenerse en la debida consideración, sobre todo, en presencia de intentos jurisprudenciales, análogos a los descritos anteriormente, dirigidos a justificar el uso de técnicas de investigación intrusiva en el ámbito privado, también con independencia de los dictados normativos.

No hay que subestimar el riesgo de que si se invierte el citado orden de prelación y es el mismo órgano judicial el que encuentra por sí mismo la regla de proporcionalidad en concreto, prescindiendo de la norma fuente[61], el mencionado canon de proporcio-

[56] Ver R. Orlandi, *Usi investigativi dei cosiddetti captatori informatici*, in *Rivista italiana di diritto e procedura penale*, 2018, p. 542.

[57] A título indicativo: A. Capone, *Intercettazioni e Costituzione: problemi vecchi e nuovi*, en *Cassazione penale,* 2017, p. 1266; Illuminati, *Libertà e segretezza delle comunicazioni*, cit., p. 3832; Signorato, *Rimodulazioni normative dell'uso investigativo del captatore informatico*, cit., p. 324.

[58] Orlandi, *Usi investigativi dei cosiddetti captatori informatici»*, cit., p. 544; Id., *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, en *Rivista italiana di diritto e procedura penale,* 2014, p. 113.

[59] Tal como afirma el Tribunal Constitucional italiano este principio constituye un requisito del sistema para cualquier medida del poder público que afecte a los derechos de la persona, a la luz del artículo 3 de la Constitución. Ver Tribunal Constitucional, 27 de febrero de 2019, núm. 24, en *Giurisprudenza costituzionale* 2019, p. 292.

[60] En este sentido Caianiello, *Il principio di proporzionalità nel procedimento penale*, en *Diritto penale contemporaneo – Rivista trimestrale*, 2014, 3-4, p. 148; G. Ubertis, *Equità e proporzionalità* versus *legalità processuale: eterogenesi dei fini?*, en *Archivio penale*, 2017, 2, p. 392.

[61] D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, en *Rivista italiana di diritto e procedura penale,* 2020, p. 27.

nalidad podría emplearse para gestionar libremente y bajo la bandera de la eficacia operativa, medios dotados de una enorme capacidad para socavar las libertades del individuo[62].

En ausencia de un estatuto normativo previo que fije distintamente los límites del ejercicio proporcionado del poder restrictivo de los derechos inviolables, el juez no está obligado a revisar si el acto intrusivo se aparta del esquema legal típico, sino las consecuencias en términos concretos producidas por la injerencia probatoria en las prerrogativas del destinatario[63]. De esa manera, se ve colocado en la condición de establecer discrecionalmente el régimen de compresión del derecho individual afectado por la acción investigadora[64].

Y – hay que decirlo – cuando falta una base jurídica sólida, la libertad de decisión cae inevitablemente en la arbitrariedad[65].

El riesgo, en esencia, es que los equilibrios de la balanza subyacente al canon de proporcionalidad acaben dependiendo sólo de la mayor o menor inclinación del magistrado a proteger las garantías individuales, en lugar del interés colectivo en la represión de los delitos.

Tampoco tranquiliza frente a tal riesgo de arbitrariedad jurisdiccional la referencia al estándar mínimo y obligatorio de protección de la esfera individual previsto en el artículo 8 CEDH, cuya operatividad en el ámbito interno como norma de rango subconstitucional[66] eleva el citado artículo al papel de parámetro orientador del juez

[62] Véase, de nuevo, Negri, *ibidem*.

[63] El concepto trascrito en el texto evoca similitudes con la deriva jurisprudencial sufrida por la declaración de nulidad de los actos procesales sobre la base de la teoría del perjuicio real de los intereses protegidos por la norma vulnerada sobre la que, por todos, véase Caianiello, *Premesse per una teoria del pregiudizio effettivo nelle invalidità processuali penali*, Bup Bologna, 2012.

[64] Ver en el mismo sentido E. Andolina, *La raccolta dei dati relativi alla localizzazione del cellulare ed al traffico telefonico tra inezia legislativa e supplenza giurisprudenziale*, en *Archivio penale web*, 2020, 3, p. 17; F. Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni rispetto ai nuovi mezzi di ricerca della prova*, en G. Dodaro-E.M. Mancuso (dirigido por), *Uguaglianza, proporzionalità e solidarietà nel costituzionalismo penale contemporaneo*, Edizioni DipLap, Milano, 2018, p. 197.

[65] Así, efectivamente, O. Mazza, *Il crepuscolo della legalità processuale al tempo del giusto processo*, en *Criminalia*, 2016, p. 336.

[66] Se hace referencia a la reconstrucción elaborada por las sentencias "gemelas" del Tribunal Constitucional italiano,

nacional llamado a afectar, con su propia medida, un derecho inviolable del individuo[67].

Es indudable que la citada disposición convencional contempla la posibilidad de injerencias autoritarias en la vida privada sólo si están previstas por la ley y constituyen una medida que, en una sociedad democrática, es necesaria [entre otras cosas] para la defensa del orden público y la prevención de los delitos. De este modo, vincula el juicio de proporcionalidad de la injerencia a la comprobación de la existencia de una disposición legal concreta que le da la base justificativa[68].

Sin embargo, es igualmente cierto que esta disposición no sólo es relevante en su dimensión literal. La garantía fijada por el citado artículo 8 del CEDH se ve, de hecho, afectada por los "humores cambiantes"[69] del Tribunal Europeo de Derechos Humanos, cuya labor hermenéutica constituye una linfa vital para los preceptos del Convenio[70]. Y, precisamente en lo que se refiere al uso investigativo de instrumentos técnicos intrusivos y de vigilancia electrónica, la jurisprudencia europea tiende a oscilar ambiguamente.

Los jueces europeos expresan a veces su firme desaprobación de las operaciones invasivas en la vida privada que no se apoyan en una base jurídica suficientemente analítica[71] o se llevan a cabo de una manera que, en la práctica, no respeta el principio de proporcionalidad[72]; otras veces consideran perfectamente compatibles con las garantías convencionales las intrusiones en la esfera individual operadas mediante intervenciones y tecnologías de vigilancia masiva funcionales a la seguridad del Estado, incluso en au-

24 de octubre de 2007, núm. 348 y 27 de octubre de 2007, núm 349, en *Giurisprudenza costituzionale,* 2008, pp. 3475 ss. y pp. 3535 ss.

[67] Ver Caianiello, *Il principio di proporzionalità nel procedimento penale*, cit., p. 159.

[68] Nicolicchia, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni rispetto ai nuovi mezzi di ricerca della prova*, cit., p. 186.

[69] Caprioli, *Tecnologia e prova penale: nuovi diritti e nuove garanzie*, cit., p. 51.

[70] A este respecto, véase Daniele, *Norme processuali convenzionali e margine di apprezzamento nazionale*, en *Cassazione penale,* 2016, p. 1690.

[71] Tribunal europeo de derechos humanos, 27 de abril de 2017, *Sommer* v. Alemania.

[72] Tribunal europeo de derechos humanos, 30 de mayo de 2017, *Trabajo Rueda* c. España; Id., 27 aprile 2017, *Sommer* c. Alemania, cit.

sencia de una autorización judicial previa del acto intrusivo[73].

Esto explica bien, por tanto, que la importación a la práctica judicial de esquemas interpretativos y decisorios propios del Tribunal Europeo de Derechos Humanos no puede ser el antídoto contra el riesgo de ataques indebidos a los derechos fundamentales derivados del ejercicio de poderes probatorios tecnológicamente insidiosos[74].

Por el contrario, la volatilidad hermenéutica de la jurisprudencia europea, que opera sin hechos, sólo sobre la base de principios[75], constituye una prueba definitiva de que no es muy conveniente confiar, caso por caso, a los jueces individuales, el papel de guardianes efectivos de los bienes individuales, fuera de un contexto normativo preciso de referencia[76].

Y esto, está claro, no implica ninguna desconfianza irreverente hacia el buen sentido y el espíritu de equidad de los órganos del poder judicial. Se trata más bien de llamar la atención sobre el sentido mismo de la inviolabilidad de los derechos fundamentales de la persona. Estos derechos, para no resolverse en meras expectativas de protección, susceptibles de un tratamiento, de vez en cuando, incluso discriminatorio, sólo pueden ser aplicados por una ley formal y ordinaria para que sean iguales para todos[77].

[73] Tribunal europeo de derechos umanos, 13 de septiembre de 2018, *Big Brother Watch* et al. v. Reino Unido; Id., 19 de junio de 2018, *Centrum för Rättvisa* v. Suecia.

[74] Para conclusiones similares, véase Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, en *Cassazione penale,* 2013, p. 372.

[75] M. Nobili, *Torbide fonti e adorati errori*, en *Critica del diritto*, 2012, p. 164.

[76] Criticando una tarea similar encomendada al juez penal, Caprioli, *Il giudice e la legge: il paradigma rovesciato*, en *Indice penale,* 2017, p. 969; Negri, *Splendori e miserie della legalità processuale. Genealogie culturali,* ethos *delle fonti, dialettica tra le corti,* en *Archivio penale web,* 2017, p. 454.

[77] En un sentido plenamente compartido, Mazza, *Il crepuscolo della legalità processuale,* cit., p. 338. Véase también, P. Ferrua, *Il giusto processo tra governo della legge ed egemonia del potere giudiziario,* en *Diritto penale e processo,* 2020, p. 13.