DIRITTO PENALE CONTEMPORANEO

DIRITTO PENALE CONTEMPORANEO

Fascicolo
11/2018

DIRETTORE RESPONSABILE Gian Luigi Gatta
VICE DIRETTORI Guglielmo Leo, Luca Luparia

ISSN 2039-1676

COMITATO DI DIREZIONE Alexander Bell, Antonio Gullo, Luca Masera, Melissa Miedico, Alfio Valsecchi

REDAZIONE Anna Liscidini (coordinatore), Alberto Aimi, Enrico Andolfatto, Enrico Basile, Carlo Bray, Alessandra Galluccio, Stefano Finocchiaro, Francesco Lazzeri, Erisa Pirgu, Serena Santini, Tommaso Trinchera, Maria Chiara Ubiali, Stefano Zirulia

COMITATO SCIENTIFICO Emilio Dolcini, Novella Galantini, Alberto Alessandri, Jaume Alonso-Cuevillas, Giuseppe Amarelli, Ennio Amodio, Francesco Angioni, Roberto Bartoli, Fabio Basile, Hervé Belluta, Alessandro Bernardi, David Brunelli, Silvia Buzzelli, Alberto Cadoppi, Michele Caianiello, Lucio Camaldo, Stefano Canestrari, Francesco Caprioli, David Carpio, Elena Maria Catalano, Mauro Catenacci, Massimo Ceresa Gastaldo, Mario Chiavario, Luis Chiesa, Cristiano Cupelli, Angela Della Bella, Gian Paolo Demuro, Ombretta Di Giovine, Massimo Donini, Giovanni Fiandaca, Roberto Flor, Luigi Foffani, Gabriele Fornasari, Loredana Garlati, Mitja Gialuz, Glauco Giostra, Giovanni Grasso, Giulio Illuminati, Roberto E. Kostoris, Sergio Lorusso, Stefano Manacorda, Vittorio Manes, Luca Marafioti, Enrico Marzaduri, Jean Pierre Matus, Anna Maria Maugeri, Oliviero Mazza, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Santiago Mir Puig, Vincenzo Mongillo, Adan Nieto Martin, Francesco Mucciarelli, Renzo Orlandi, Íñigo Ortiz de Urbina, Francesco Palazzo, Claudia Pecorella, Marco Pelissero, Vicente Pérez-Daudí, Daniela Piana, Lorenzo Picotti, Paolo Pisa, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Joan Josep Queralt, Tommaso Rafaraci, Paolo Renon, Mario Romano, Gioacchino Romeo, Carlo Ruga Riva, Markus Rübenstahl, Francesca Ruggieri, Marco Scoletta, Sergio Seminara, Rosaria Sicurella, Placido Siracusano, Carlo Sotis, Giulio Ubertis, Antonio Vallini, Paolo Veneziani, Francesco Viganò, Costantino Visconti, Matteo Vizzardi, Francesco Zacchè

Diritto Penale Contemporaneo è un periodico on line, ad accesso libero e senza fine di profitto, nato da un'iniziativa comune di Luca Santa Maria, che ha ideato e finanziato l'iniziativa, e di Francesco Viganò, che ne è stato sin dalle origini il direttore nell'ambito di una partnership che ha coinvolto i docenti, ricercatori e giovani cultori della Sezione di Scienze penalistiche del Dipartimento "C. Beccaria" dell'Università degli Studi di Milano. Attualmente la rivista è edita dall'Associazione "Diritto penale contemporaneo", il cui presidente è l'Avv. Santa Maria e il cui direttore scientifico è il Prof. Gian Luigi Gatta. La direzione, la redazione e il comitato scientifico della rivista coinvolgono oggi docenti e ricercatori di numerose altre università italiane e straniere, nonché autorevoli magistrati ed esponenti del foro.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
Le opere pubblicate su "Diritto penale contemporaneo" sono attribuite dagli autori con licenza *Creative Commons* "Attribuzione – Non commerciale 3.0" Italia (CC BY-NC 3.0 IT). Sono fatte salve, per gli aspetti non espressamente regolati da tale licenza, le garanzie previste dalla disciplina in tema di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (l. n. 633/1941).
Il lettore può condividere, riprodurre, distribuire, stampare, comunicare al pubblico, esporre in pubblico, cercare e segnalare tramite collegamento ipertestuale ogni lavoro pubblicato su "Diritto penale contemporaneo", con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza *Creative Commons* "Attribuzione – Non commerciale 3.0 Italia" (CC BY-NC 3.0 IT), in particolare conservando l'indicazione della fonte, del logo e del formato grafico originale, nonché dell'autore del contributo.
La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

***Peer review*.**
Salvo che sia diversamente indicato, tutti i contributi pubblicati nella sezione *papers* di questo fascicolo hanno superato una procedura di *peer review*, attuata secondo principi di trasparenza, autonomia e indiscusso prestigio scientifico dei revisori, individuati secondo criteri di competenza tematica e di rotazione all'interno dei membri del Comitato scientifico. Ciascun lavoro soggetto alla procedura viene esaminato in forma anonima da un revisore, il quale esprime il suo parere in forma parimenti anonima sulla conformità del lavoro agli standard qualitativi delle migliori riviste di settore. La pubblicazione del lavoro presuppone il parere favorevole del revisore. Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione.
Per la citazione dei contributi presenti nei fascicoli di *Diritto penale contemporaneo*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Dir. pen. cont.*, fasc. 1/2017, p. 5 ss.

11/2018

L'ODISSEA DEL *TROJAN HORSE*

Tra potenzialità tecniche e lacune normative

di Oscar Calavita

Abstract. *Con il d.lgs. 29 dicembre 2017, n. 216 – pubblicato in Gazzetta Ufficiale 11 gennaio 2018, n. 8 – il Governo ha dato seguito alla delega legislativa attribuitagli dall'art. 1, comma 84, l. 23 giugno 2017, n. 103. Il presente contributo intende focalizzare l'attenzione precipuamente sulla neointrodotta disciplina legislativa del captatore informatico, anche alla luce del diritto pretorio che si era creato in precedenza all'emanazione del decreto delegato e cristallizzato nelle Sezioni Unite Scurato.*

1. Premessa.

Le nuove tecnologie, in particolare con l'avvento di internet, stanno caratterizzando la vita di ogni consociato, si evolvono a ritmi serrati e si sono ormai radicate nel quotidiano di ognuno di noi[1]: da quando ci si sveglia e sino al termine della giornata non facciamo altro che venire in contatto con strumenti tecnologici di ultima generazione. Si pensi, per fare qualche esempio, agli *smartphone*, ai pc utilizzati sia per svago sia per lavoro, nonché agli ultimi modelli di automobile che incorporano sistemi GPS all'avanguardia e possono connettersi con i cellulari: e l'elenco potrebbe estendersi quasi all'infinito.

È indiscutibile che, grazie (o a causa) delle nuove tecnologie, i rapporti sociali siano mutati e si siano adattati ai tempi, fornendo certamente un grande contributo per

[1] Anche del giurista, il quale «da giurista umanista tende ad assumere le vesti di "giurista tecnologico"» (S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018, p. 11).

mettere in contatto persone da ogni parte del mondo per mezzo dei *social network*. Tuttavia, come ogni strumento inventato per fornire un contributo all'uomo, vi è sull'altro piatto della bilancia la sempre pendente spada di Damocle dell'illegalità, pronta ad abbattersi inesorabilmente a perseguire fini criminosi e ledere i diritti fondamentali dell'individuo[2].

Se è vero che gli strumenti informatici possono essere utilizzati per commettere determinati tipi di reato o agevolarne la commissione, d'altro canto non può non notarsi come anche la Procura della Repubblica abbia a disposizione internet, nuove tecnologie e le indagini digitali[3] nella lotta alla repressione delle manifestazioni delittuose[4].

In particolare, negli ultimi anni si è ingerito nel panorama investigativo con sempre maggiore frequenza il captatore informatico, un *software* (*rectius*: *malware*[5]) di tipo *trojan* che si introduce occultamente nelle "mura protette" di un sistema informatico, così come «l'agguato del caval»[6] permise ai greci di penetrare le invalicabili mura della città di Ilio[7].

Sul punto, nonostante ancora non si presentasse sullo scenario internazionale la figura del virus informatico, già nel 2001 la Convenzione sul *cybercrime*[8] del Consiglio

---

[2] V. anche P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Processo penale e giustizia*, 5, 2016, p. 2, secondo cui «l'avvento dell'era digitale ha prodotto nuove minacce criminali e ha modificato la fisionomia delle forme di manifestazione della delinquenza determinando una crescita esponenziale della frequenza con cui gli illeciti comuni sono compiuti attraverso lo strumento digitale».

[3] «Con la locuzione "indagini digitali" si può indicare qualunque tipologia investigativa che impieghi la tecnologia digitale, indipendentemente dal tipo di reato perseguito, che potrebbe essere sia informatico, sia cibernetico, sia comune» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 44).

[4] Sul punto vedansi le osservazioni formulate da P. TONINI, *I captatori informatici*, in *Jusonline*, 3, 2017, p. 380. Secondo l'Autore, le nuove tecnologie investigative possono suscitare sentimenti diametralmente antitetici, da chi ne prova repulsione a chi, al contrario, ne comprende le potenzialità e ne accoglie i benefici, dal momento che «la criminalità sfrutta gli strumenti esistenti, che assicurano l'inaccessibilità delle comunicazioni e delle conversazioni». Oltre alla dicotomia sentimentale, secondo la dottrina citata le nuove tecnologie pongono all'interprete almeno quattro interrogativi: 1) in quale categoria giuridica sono sussumibili i nuovi strumenti tecnici? 2) quali beni giuridici vengono in gioco? 3) quali sono i principi utilizzabili per superare i contrasti che possono andare creandosi? 4) «come il giurista deve trattare la prova acquisita mediante captatore»?

[5] Secondo la definizione riportata dal *Cambridge Dictionary*, «a *Malware is a software that is designed to damage the information on other people's computers, and prevent the computers from working normally*»; «*Malware is short for "malicious software" and is a catch-all term for viruses, spyware, worms, browser hijackers, etc*».

[6] D. ALIGHIERI, *Divina commedia. Inferno, canto XXVI, v. 59*.

[7] In dottrina si è evidenziato, con metafora epica, che «il virus *trojan* prende il suo nome, verosimilmente, dal leggendario cavallo di Troia che, per mezzo di Odisseo, l'uomo dal multiforme ingegno, riuscì ad entrare dentro le mura di Troia, con inganno, ed espugnarla. Così come il cavallo di Troia sconfisse i troiani entrando all'interno della loro cittadella muraria, fingendosi un dono pregiato da parte degli Achei, così anche il predetto virus riesce ad entrare, con inganno, nell'apparecchio […] che si vuole intercettare, non per distruggerlo né tanto meno per danneggiarlo, ma per carpire qualsiasi dato che ivi possa trovarvi» (M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, in questa *Rivista*, fasc. 2/2018, p. 23).

[8] I *cybercrimes* sono una sola delle due ampie categorie che possono essere ricondotte alla settore della disciplina penalistica definita "diritto penale dell'informatica": accanto ad essi, infatti, si affiancano i *computercrimes*. Questi ultimi si caratterizzano per lo strumento con il quale vengono commessi (*i.e.*

d'Europa, siglata a Budapest il 23 novembre dello stesso anno, aveva disegnato all'art. 15 una nutrita serie di principi minimi processuali ai quali le legislazioni statali avrebbero dovuto adeguarsi: (1) riserva di legge; (2) tutela della dignità della persona[9]; (3) riserva di giurisdizione, o quantomeno la supervisione di un organo indipendente; (4) principio di proporzionalità, secondo il quale il sacrificio imposto alla libertà personale di un soggetto deve essere proporzionato e adeguato al reato che si vuole perseguire.

Inoltre, come corollario dei principi generali appena enunciati, nella medesima sezione II dedicata al diritto procedurale, la Convenzione detta un eterogeneo coacervo di disposizioni relative a modalità di ricerca e acquisizione della prova[10], alle quali il legislatore si era allineato con l'emanazione della legge di ratifica della Convenzione di Budapest 18 marzo 2008, n. 48. Lo Stato italiano, però, «con una operazione di cinico pragmatismo»[11] e con eccesiva timidezza, non aveva introdotto alcun nuovo mezzo di ricerca della prova, limitandosi ad adattare le discipline previgenti all'incessante avanzare tecnologico[12].

Se già, tuttavia, dieci anni or sono la legislazione sembrava rincorrere l'avanzare tecnologico[13], l'avvento del captatore informatico ha posto nuove sfide esegetiche che ancora oggi non si sono sopite. Invero, è innanzitutto fondamentale comprendere le potenzialità tecniche del virus; se vi sono nuovi diritti che possono essere lesi con le potenzialità intrusive del *trojan horse*, ovvero se l'elencazione di quelli già annoverati nella Carta costituzionale siano sufficienti[14]; conseguentemente valutare se le operazioni

---

l'informatica); mentre i primi si distinguono per un utilizzo del *web* a fini criminosi. Sul punto v. *amplius* S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 41 s.

[9] «Ogni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani» (art. 15, §1, Convenzione di Budapest).

[10] «Conservazione rapida di dati informatici immagazzinati (art. 16), «conservazione e divulgazione rapide di dati relativi al traffico (art. 17), «ingiunzione di produrre» (art. 18), «perquisizione e sequestro di dati informatici immagazzinati» (art. 19), «raccolta in tempo reale di dati sul traffico» (art. 20), «intercettazioni di dati relativi al contenuto» (art. 21).

[11] S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 02, 2015, p. 766.

[12] L'opera di *lifting* del codice di procedura penale è stata apportata dagli artt. 8, 9 e 11 della l. 48/2008, che rispettivamente hanno modificato alcune norme del Libro III, del libro IV e l'art. 51 c.p.p.

[13] In particolare ci si riferisce alla raccolta in tempo reale dei dati sul traffico, poiché tale modalità investigativa, «benché "tipica" sul versante internazionale, perché descritta dalla Convenzione, resta "atipica" sul versante interno, perché non prevista da nessuna norma, non potendosi certo valorizzare in tal senso la generica locuzione di piena ed intera esecuzione data alla Convenzione, contenuta nell'art, 2 della legge n. 48 del 2008» (S. MARCOLINI, *Le indagini atipiche*, op. cit., p. 766).

[14] F. RUGGIERI, *L'impatto delle nuove tecnologie: il captatore informatico. L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, in *Jusonline*, 3, 2017, p. 371 ritiene non necessario procedere all'enucleazione di nuovi diritti fondamentali, come teorizzato dal *Bundesversassungsgericht* nel 2008 in ordine al *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* (il

tecnico-informatiche del captatore siano ascrivibili a fattispecie tipiche investigative e/o se è possibile ricondurle nell'alveo delle indagini atipiche ai sensi dell'art. 189 Cost. Svolte tali premesse, il contributo vuole focalizzare l'attenzione sullo stato dell'arte precedente all'emanazione del d.lgs. 29 dicembre 2017, n. 216, lasciato alla nomopoiesi giurisprudenziale, per poi evidenziare i limiti della nuova normativa.

2. Le potenzialità tecniche del captatore informatico.

Il peculiare strumento intercettivo costituito dal captatore informatico[15], il cui ambito applicativo, negli ultimi anni, scevro di una disciplina legislativa di riferimento, era stato demandato evoluzione giurisprudenziale[16], conosce una sempre più frequente impiego da parte degli inquirenti.

Infatti, il *trojan horse*[17] utilizza una tecnica informatica conosciuta come *Remote Control System* (RCS), la quale – come si evince dalla definizione – permette un controllo totale da remoto del sistema infettato[18], consentendo così agli investigatori di acquisire

---

diritto all'integrità e riservatezza dei sistemi informatici), a condizione che sia garantito il rispetto della doppia riserva legislativa e giurisdizionale. Ritiene di estendere la tutela del domicilio fisico a quella del domicilio informatico S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 49 ss.

[15] Il captatore informatico è stato definito dalla dottrina come un *malware* «occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva […], il quale consente in ogni momento all'attaccante […] di captare tutto il traffico dati (sia in entrata sia in uscita), di attivare da remoto il microfono e la telecamera registrando le attività, di perquisire gli *hard disk* e di fare copia integrale del loro contenuto, di intercettare tutto quanto digitato sulla tastiera, di fotografare le immagini e i documenti visualizzati» (L. ANNUNZIATA, Trojan *di Stato: l'intervento delle Sezioni Unite non risolve le problematiche applicative connesse alla natura del captatore informatico*, in AA. VV., Trojan horse*: tecnologia, indagini e garanzie di libertà (profili di* intelligence*)* in *www.parolaalladifesa.it*, 06 settembre 2016, p. 189). Ancora: il «*trojan horse* potremmo dire che è un *software* malevolo che maschera la sua vera identità al fine di sembrare per il funzionamento del dispositivo o comunque interessante per l'uso che l'utente ne potrebbe fare» (M. ZONARO, *Aspetti tecnici e operativi per l'utilizzo di un innovativo strumento di intercettazione*, in AA. VV., Trojan horse*: tecnologia, indagini e garanzie di libertà (profili di* intelligence*)*, in *www.parolaalladifesa.it*, 06 settembre 2016, p. 165.

[16] V. *ex multis* Cass., Sez. V, 14 ottobre 2009, 16556, Virruso, in *CED* n. 246954; Cass., Sez. VI, 26 maggio 2015, n. 27100, Musumeci, in *CED* n. 265654; Cass., Sez. VI, 03 maggio 2016, n. 27404; Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato; Cass., Sez. V, 30 maggio 2017, n. 48370; Cass., Sez. V, 09 febbraio 2018, n. 15288; Cass., Sez. III, 28 febbraio 2018, n. 28516 (le sentenze e le relative massime sono state ricavate dai seguenti siti: *www.iusexplorer.it*, *www.pluris-cedam.utetgiuridica.it*, *www.cortedicassazione.it*).

[17] Denominato anche virus informatico, virus *trojan*, captatore informatico, agente intrusore, virus di stato. Secondo altri, invece, «più corretta, tra quelle utilizzate in giurisprudenza, appare, pertanto, quella di "agente intrusore informatico" in quanto fa perno su tre concetti semplici e diretti: l'agire, l'intrusione, l'àmbito informatico» (D. MINOTTI, *Captatore informatici: per un ponte tra diritti e informatica*, in AA. VV., Trojan horse*: tecnologia, indagini e garanzie di libertà (profili di* intelligence*)* in *www.parolaalladifesa.it*, 06 settembre 2016, p. 168).

[18] Secondo parte della dottrina, le potenzialità tecniche del captatore informatico consento non solo il monitoraggio in tempo reale del dispositivo bersaglio, bensì anche di terzi apparecchi allo stesso collegati da una rete LAN. In altre parole, l'agente intrusore «può monitorare pure i dispositivi, anche appartenenti terzi, che siano collegati mediante una rete locale al dispositivo informatico su cui è stato installato il *trojan*» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 239).

un ampio materiale conoscitivo, potenzialmente consistente in ogni atto quotidiano della vita di un soggetto. Sono dunque svariate le funzionalità che si possono ricavare dal captatore legale, un «"bulimico" congegno»[19] inoculabile all'interno di qualsiasi dispositivo *target* – portatile e fisso – dotato di una connessione *internet*, sia essa *wi-fi* sia essa *ethernet*[20]. Come brillantemente evidenziato dalla giurisprudenza[21] e dalla dottrina[22], con il captatore informatico è possibile svolgere un'eterogenea congerie di attività tipiche e atipiche di indagine pesantemente intrusive delle libertà del soggetto destinatario, eziologicamente volte, come una sorta di "*panopticon* benthamiano", a sorvegliare ogni atto quotidiano della vita[23]. Infatti, con il captatore – che sfugge ad oggi ad ogni antivirus in commercio e destinato a divenire ben presto obsoleto se non aggiornato e/o modificato costantemente[24] – è possibile, tra il resto:

1) attivare il microfono, intercettando le comunicazioni che avvengono tra i presenti nella portata del raggio del dispositivo *target*[25];

---

[19] L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in AA. VV., Trojan horse*: tecnologia, indagini e garanzie di libertà (profili di* intelligence*)*, in *www.parolaalladifesa.it*, 06 settembre 2016, p. 180.

[20] A titolo esemplificativo si possono citare gli *smartphone*, *tablet*, PC, *laptot*, *Smart* TV, autovetture e, più in generale, qualsiasi dispositivo dotato di tecnologia *Smart*.

[21] Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, op. cit.

[22] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, pp. 483-510; D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *Jusonline*, 3, 2017, p. 385; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in questa *Rivista*, fasc. 1/2018, p. 216; S. SIGNORATO, *Le indagini digitali*, op. cit., p. 239; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, Milano, 2017, p. 18; Inoltre, secondo G. ZICCARDI, *Parlamento Europeo, captatore informatico e attività di* hacking *delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche*, in *Arch. pen*., 1, 2017, p. 1, le operazioni tecniche effettuabili per mezzo dell'agente intrusore potrebbero suddividersi in tre macro-aree, riconducibili 1) al controllo dell'*hardware* del dispositivo; 2) al controllo dei contenuti del dispositivo; 3) all'acquisizioni di informazioni scambiate sul dispositivo. A ben vedere, tuttavia, le ultime due funzioni potrebbero essere lette quale *species* del *genus* di cui al punto n. 1.

[23] In dottrina v. P. TONINI, *I captatori informatici*, op. cit., p. 379, secondo cui «il captatore informatico e le perquisizioni *on line* hanno una capacità invasiva totale sulla vita delle persone».

[24] Sostiene M. TORRE, *Il captatore informatico*, op. cit., p. 17, che «non esiste, infatti, un unico *software*, ma diversi programmi tecnicamente in grado di carpire i dati e le informazioni dei dispositivi bersaglio. Tali programmi, peraltro, lungi dall'avere una lunga vita operativa, sono destinati all'obsolescenza precoce, dovendosi adeguare in tempo reale al continuo sviluppo della tecnologia difensiva (*antivirus*) in grado di bloccare sul nascere i tentativi di infiltrazione dei *virus*, anche quelli di Stato». Si è, in sostanza, alla presenza di una continua rincorsa tra virus e antivirus: una corsa tecnologica che porterà a un livello sempre maggiore di affidabilità dei sistemi e di virus sempre più invasivi. In altre parole, si può affermare che si è in presenza di una hegeliana dialettica tra sistemi, in cui alla tesi (il virus) segue l'antitesi (l'antivirus), per giungere alla sintesi (il nuovo virus in grado di penetrare le difese dell'antivirus precedente): e così potenzialmente ciclicamente sino all'infinito.

[25] Se la dottrina (pare) maggioritaria (v., per tutti, M. TORRE, *Il captatore informatico*, op. cit.) e la giurisprudenza, già prima della novella legislativa, non trovavano ostacoli nel ricondurre l'intercettazione itinerante alla disciplina delle intercettazioni tra presenti *ex* art. 266, comma 2, c.p.p.; altri al contrario sostenevano che «a ben vedere, proprio dalla premessa da cui muovono le Sezioni Unite, secondo cui il giudice non può previamente conoscere il domicilio intercettato, deriva l'ovvia conclusione per cui la ispe-

2) azionare la *webcam*, ottenendo così la possibilità di realizzare *videoclip* e scattare fotografie, o solamente vedere attraverso l'occhio della telecamera;
3) captare il traffico dati, sia in arrivo sia in partenza dal dispositivo, sia esso relativo alla navigazione sia esso concernente la posta elettronica (*web mail* e *out look*);
4) prendere visione di ciò che appare sullo schermo (*screenshot*[26] e *screencast*[27]) o digitato sulla tastiera (*keylogger*);
5) perquisire l'*hard disk* ed estrarne copia, totale o parziale;
6) tracciare la posizione GPS.

A tali funzionalità deve aggiungersi la possibilità di "intercettare" – in senso atecnico – anche le comunicazioni che vengono effettuate per mezzo dei più diffusi applicativi di messaggistica istantanea, i quali consentono non solo lo scambio di messaggi, bensì anche di immagini, video, *link* etc.[28]. Tali applicazioni, a differenza delle tradizionali intercettazioni telefoniche che richiedono la collaborazione del gestore di telefonia che sdoppia il segnale comunicativo e lo dirama anche verso gli uffici di Procura[29], si appoggiano sulla linea internet che prescinde totalmente da qualsiasi rapporto con l'operatore. Infatti, «la navigazione in internet avviene grazie ad un meccanismo di "impacchettamento" delle informazioni che poi vengono inviate a destinazione; ogni singolo pacchetto di dati contiene al suo interno sia "l'indirizzo" del mittente che quello del destinatario»[30], il quale può essere criptato o meno: nel primo

---

perqui-intercettazione "itinerante", al pari delle riprese visive, non è prevista dalla legge, né è sottoponibile al previo controllo giurisdizionale quanto agli ignoti domicili che potranno essere violati, sottraendosi così alla "doppia riserva" di legge e di giurisdizione, imposta dagli artt. 14 e 15 Cost., oltre che dall'art. 8 C.E.D.U.» e che, di conseguenza, «trattandosi di un mezzo di ricerca della prova non previsto dalla legge, la violazione del principio di legalità processuale rende questa tecnologia investigativa non una prova atipica, ma una prova "incostituzionale" e "inconvenzionale", perché darebbe luogo ad un'inammissibile autorizzazione ad una ispe-perqui-intercettazione "in bianco", cioè "in qualsiasi domicilio» (L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante"*, op. cit., p. 180).

[26] Lo *screenshot* è una fotografia dello schermo del dispositivo, che può altresì essere programmato a intervalli di tempo regolari per un controllo costante del bersaglio.

[27] Lo *screencast* è una registrazione digitale dell'*output* dello schermo. In sostanza è un video di quanto avviene sullo schermo del dispositivo bersaglio, il quale può ricavarsi anche da una programmazione con una frequenza incalzante di *screenshot*.

[28] Un quadro di insieme dei programmi criptati maggiormente usati e disponibili gratuitamente negli *AppStore* è dato da M. TORRE, *Il captatore informatico*, op. cit., p. 22 (nota n. 2), nonché da M. DI STEFANO-B. FIAMMELLA, *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (profili di* intelligence), Altalex, Milano, 2015: *Whatsapp, Telegram, Skype, Snapchat, Messenger, Instagram, Twitter, Wechat, WebPhone, Gmail, My-B-Line, PowerVoip, uVOIPit, Lingo, VoiPax, Wor(l)d softSim, Viber, vBuzzer, VoipBuster, MOBIVOX, Line2, Skebby, MyCallingBox, InTouchApp, Miglu, Voxtopia, Poketalk, Fring, EvaPhone, PC-Telephone, Rebtel, VoxOx, Vyke, Yahoo Voice, FriendCaller, FaceTime, MagicJack, Vonage, Google Voice, Tru, Vopium, Call, ooVoo, JAJAH*.

[29] «Lo stesso concetto è valido per tutte le intercettazioni di conversazioni tra presenti, sia che avvengano con microspie funzionanti su rete radiomobile GSM/UMTS (come se fossero dei normali telefoni cellulari), sia che vengano captate con microspie digitali in radiofrequenza, il cui segnale venga poi instradato su rete telefonica» (M. ZONARO, *Aspetti tecnici e operativi*, op. cit., p. 164).

[30] M. ZONARO, *Aspetti tecnici e operativi*, op. cit., p. 164.

caso non vi è la possibilità di intercettare il contenuto del "pacchetto dati", bensì essere semplicemente a conoscenza dell'esistenza dello stesso; nel secondo caso la mancata criptazione permette anche di prendere visione del contenuto. Le società che gestiscono i *social network* ricorrono alla criptazione dei dati dei loro utenti, al fine di garantirne la riservatezza da possibili intrusioni esterne[31]. È per questo motivo, non potendo ricorrere alle intercettazioni tradizionali, le quali al più consentono di sapere se i dispositivi in uso all'indagato sono effettivamente utilizzati, che si è sviluppata una tecnica di «intercettazione attiva»[32] attuata per il mezzo del captatore informatico. In sostanza, gli inquirenti, con i nuovi applicativi di messaggistica, non possono più procedere a un mero ascolto passivo, tramite la captazione di un flusso di dati, delle comunicazioni intercorrenti tra due utenze telefoniche; al contrario dovranno introdursi – con l'inganno – all'interno del dispositivo ove possono prendere visione delle conversazioni criptate, dal momento che all'interno dello stesso esse risultano in chiaro.

L'installazione del *malware* utilizza due differenti moduli, un *client* e un *server*: il primo consente di controllare da remoto il dispositivo infettato, mentre il secondo è il programma che viola le difese del sistema informatico e si installa nel bersaglio. Quest'ultimo, agendo come un vero e proprio cavallo di Troia, viene solitamente installato da remoto con la necessaria collaborazione dell'ignaro bersaglio. Invero, il *server* si maschera da applicazione di uso comune – come un aggiornamento del sistema operativo, un *upgrade* di una applicazione o una banale mail – che, a prima vista, non può essere dannosa per il dispositivo. Il bersaglio, perciò, è indotto a dare seguito all'operazione richiesta dal sistema informatico, nell'erronea convinzione che la componente a lui nota sia innocua; ancor più semplice risulta essere l'inoculazione del *virus* qualora il *target* abbia tra le impostazioni di *default* l'aggiornamento automatico del sistema[33]. Tuttavia, il programma noto cela al proprio interno una funzionalità sconosciuta che consente di creare una «*backdoor*», la quale permette di aprire «una o più porte di comunicazione del dispositivo stesso verso il server d'ascolto, […] consentendo così il controllo dell'apparato»[34-35].

---

[31] In dottrina è stato portato l'esempio del colosso dell'informatica *Google*, il quale ha resistito al tentativo del Governo degli Stati Uniti d'America di ottenere informazioni riservate degli utenti del motore di ricerca (v. P. TONINI, *I captatori informatici*, op. cit., p. 380).

[32] M. TORRE, *Il captatore informatico*, op. cit., p. 24.

[33] Agendo in tale modo, secondo parte della dottrina si sarebbe in presenza di una attività investigativa a «fattispecie complessa, che ricomprende per un verso l'attività dell'organo investigatore, ma per l'altro anche quella dell'indagato» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 238). Quest'ultima attività, peraltro, secondo la stessa dottrina potrebbe porsi in contrasto con il principio del *nemo tenetur se detegere – lato sensu* inteso quale diritto a non porre in essere comportamenti autoincriminanti –, dal momento che un simile comportamento tenuto dall'indagato finisce necessariamente con il riflettersi in una collaborazione a lui deleteria.

[34] M. ZONARO, *Aspetti tecnici e operativi*, op. cit., p. 165. Inoltre, secondo lo stesso Autore «contrariamente a quanto fanno molti virus e *worm*, i *Trojan* non tentano di iniettarsi in altri file o di propagarsi su altri dispositivi. Il controller, una volta andata a buon fine l'inoculazione del *Trojan*, agisce dal proprio computer inviando al dispositivo infettato istruzioni specifiche».

[35] Per semplificare con un esempio, il server ha una duplice natura. Da un lato è visto come il cavallo donato agli abitanti della città di Troia, apparentemente innocuo. Dall'altro, invece, cela al proprio interno i soldati

Altro *modus operandi*, di gran lunga più rischioso per la segretezza delle indagini e per l'incolumità degli operanti, è l'iniezione del virus informatico direttamente e fisicamente sul *hardware* del bersaglio che, tuttavia, deve rimanere incustodito e tale da consentirne un'aggressione da parte degli organi di P.G.[36]: anche in questo caso, quindi, seppur indirettamente, vi deve essere la collaborazione del soggetto passivo[37].

Come visto in precedenza, svariate sono le funzionalità che si possono operare con il captatore informatico. Ad avviso di parte della dottrina[38], la congerie di potenzialità tecniche può essere raggruppata in due macro aree riconducibili alla *online search* e alla *online surveillance*.

La prima consente di perquisire da remoto il contenuto del *hard-disk* e di farne copia totale o parziale. Da notare che il codice di rito prevede espressamente il sequestro del corpo del reato e delle cose pertinente al reato necessarie all'accertamento dei fatti (art. 253 c.p.p.): se il corpo del reato o le cose pertinenti al reato sono degli oggetti informatici (per esempio un pc) è dunque possibile estrapolarne la copia del contenuto ai sensi dell'art. 258 c.p.p., ma solamente in seguito a un sequestro probatorio della fisicità del dispositivo, cosicché la perquisizione non avviene a distanza[39]. Diversamente, la perquisizione da remoto – benché persegua il medesimo fine della copia integrale del contenuto del *target* – non è disciplinata in alcuna norma del codice di rito e – a meno di non ricorrere all'argomentazione analogica, vietata nel caso di specie perché incide sulle garanzie dei diritti fondamentali – non può essere legittimamente utilizzata quale mezzo di indagine[40]: inammissibile, quindi, allo stato dell'arte, pare essere la tecnica di intercettazione attiva dei messaggi *Whatsapp* sopra citata.

Dal canto loro, le tecniche di *online surveillance*, che permettono un controllo in tempo reale di tutto ciò che avviene sul dispositivo *target* (*screenshot*, *screencast*, *keylogger*, intercettazioni ambientali) parevano essere «riconducibili contenutisticamente a istituti codicistici»[41], sicché venivano ad essere sussunte, in linea generale, nella disciplina delle

---

che, nottetempo, consentirono la disfatta della fortezza dell'Ellesponto.

[36] V. *amplius* A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Cedam, Padova, 2015, p. 84.

[37] Riassume i rischi evitabili (dal) e i vantaggi del captatore informatico F. PERNA, *Il Captatore informatico nell'attuale panorama investigativo: riflessi operativi*, in AA. VV., Trojan horse*: tecnologia, indagini e garanzie di libertà (profili di* intelligence*)*, in *www.parolaalladifesa.it,* 06 settembre 2016, p. 172: «non solo la fase di studio delle abitudini dell'indagato – indispensabile per la collocazione degli apparati di captazione – potrebbe in prospettiva ridursi in maniera significativa, ma l'esposizione del personale operante, nonché le imprevedibili *discovery* legate alla casualità e allo stesso intervento umano potrebbero essere addirittura eliminate».

[38] P. FELICIONI, *L'acquisizione da remoto*, op. cit., p. 123; M. GRIFFO, *Una proposta costituzionalmente orientata*, op. cit., p. 24; E.M. MANCUSO, *La perquisizione on-line*, in *Jusonline*, 3, 2017, pp. 414 ss.; M. TORRE, *Il captatore informatico*, op. cit., p. 18.

[39] Conferma da ultimo tale impostazione Cass., Sez. III, 23 giugno 2015, n. 38148.

[40] «Tale inedito sviluppo investigativo – perquisizione dell'*hard disk* per fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira – non conosce alcuna regolamentazione né a livello di diritto positivo né a livello di diritto pretorio» (M. TORRE, *Il captatore informatico*, op. cit., p. 56). Le considerazioni appena esposte, benché formulate in un momento antecedente la delega Orlando, valgono anche in seguito alla riforma intervenuta in seguito all'emanazione del d.lgs. 216/2017.

[41] P. FELICIONI, *L'acquisizione da remoto*, op. cit., p. 125.

intercettazioni telematiche (art. 266 *bis* c.p.p.) e delle intercettazioni di comunicazioni tra presenti (art. 266 c.p.p.). Ad oggi, però, in seguito alla presa di posizioni delle Sezioni Unite Scurato e del decreto legislativo 29 dicembre 2017, n. 216, l'intercettazione ambientale itinerante è l'unica che trova riscontro nel codice di rito, cosicché ci si dovrà domandare, in seguito all'analisi della disciplina codicistica, se possano ritenersi ammissibili, al pari delle tecniche di *online search*, le operazioni di sorveglianza in tempo reale[42].

3. Le Sezioni Unite Scurato.

Nel *mare magnum* delle potenzialità applicative del captatore informatico, la Corte di Cassazione a Sezioni Unite[43] era stata chiamata, prima delle modifiche apportate al codice di rito dal d.lgs. 216/2017, a pronunciarsi sulla necessità, o meno, di indicare nel decreto autorizzativo dell'intercettazione virale-itinerante i luoghi in cui la captazione sarebbe stata disposta.

Nel caso di specie, la Suprema Corte era stata adita da un indagato (tra l'altro) di associazione a delinquere di stampo mafioso, il quale era ricorso avverso l'ordinanza del Tribunale delle Libertà di Palermo che confermava l'applicazione della custodia cautelare in carcere nei propri confronti, ricavando la sussistenza dei gravi indizi di colpevolezza tramite intercettazioni ambientali itineranti (anche) domiciliari effettuate con l'ausilio del virus informatico.

Per quanto qui di interesse, i motivi di doglianza risiedevano in una presunta violazione dell'art. 266, comma 2, c.p.p., posto che le intercettazioni erano state effettuate in luoghi di privata dimora[44], all'interno dei quali non vi era un fondato motivo di

---

[42] Fornisce riposta negativa al quesito P. TONINI, *I captatori informatici*, op. cit., pp. 375 s., il quale basa la propria argomentazione sul «principio di non sostituibilità» fatto proprio da Cass., Sez. Un., 28 maggio 2003, Torcasio, in *CED* n. 225467. Da ultimo v. Cass., Sez. V, 27 marzo 2015, n. 36080, Sollecito, §4.3.2: «quando il codice stabilisce un divieto probatorio oppure un'inutilizzabilità espressa, è vietato il ricorso ad altri strumenti processuali, tipici od atipici, finalizzati ad aggirare surrettiziamente un simile sbarramento».

[43] Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, op. cit. Di seguito i due principi di diritto enunciati dalla predetta sentenza: (1) «deve escludersi la possibilità di compiere intercettazioni nei luoghi indicati dall'art. 614 c.p., con il mezzo indicato, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'art. 13, d.l. 13 maggio 1991, n. 152, convertito in l. 12 luglio 1991, n. 203, non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'art. 266, comma 2, c.p.p., che in detto luogo "si stia svolgendo l'attività criminosa"»; (2) «è invece consentita la captazione nei luoghi di privata dimora *ex* art. 614 c.p., pure se non singolarmente individuati e se ivi non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica», secondo la previsione dell'art. 13 d.l. 13 maggio 1991, n. 152.

[44] Sulla nozione di «privata dimora» v. da ultimo Cass., Sez. Un., 22 giugno 2017, n. 31345, in *CED* n. 270076, che, chiamata a pronunciarsi sull'estensione della detta locuzione in un caso di furto in abitazione *ex* art. 624 *bis* c.p., ha sottolineato come detti luoghi siano quelli «nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare, compreso quelli destinati ad attività lavorativa o professionale». Per una concisa, quanto precisa, ricostruzione storica della nozione di privata dimora v. T. ALESCI, *Le intrusioni* inter praesentes, in T. BENE (a cura di),

ritenere che si stesse svolgendo l'attività criminosa, e poiché non erano stati indicati, nel provvedimento autorizzativo, i luoghi in cui l'attività captativa si sarebbe svolta.

Tale ultimo motivo di doglianza trovava supporto nella sentenza Musumeci, a detta della quale «il decreto autorizzativo deve individuare, con precisione, i luoghi nei quali dovrà essere espletata l'intercettazione delle comunicazioni tra presenti, non essendo ammissibile un'indicazione indeterminata o addirittura l'assenza di ogni indicazione al riguardo»[45], al fine di non incorrere in una lettura incostituzionale dell'art. 266 c.p.p. per violazione dell'art. 15 Cost[46].

Disattendeva una simile ricostruzione ermeneutica la medesima Sezione Sesta della Corte di Cassazione che, a un anno di distanza dalla citata sentenza Musumeci, poneva all'attenzione delle Sezioni Unite il seguente quesito nomofilattico: «se – anche nei luoghi di privata dimora *ex* art. 614 c.p., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa – sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispostivi elettronici portatili»[47].

Le Sezioni Unite, nell'«assordante silenzio»[48] legislativo, hanno così affrontato il tema delle intercettazioni tra presenti mediante l'utilizzo di un virus informatico, descrivendone le ampie capacità intrusive nella sfera privata e, al contempo, evidenziandone le potenzialità fornite alla Procura della Repubblica nella lotta contro il crimine, nonché focalizzando l'attenzione, in via preliminare, sui progetti di riforma pendenti *illo tempore* in Parlamento[49].

Svolte tali premesse, la Cassazione si è soffermata sul tema delle intercettazioni ambientali, così definite dalla dottrina e dalla giurisprudenza ma che non trovano riscontro lessicale nel codice di rito. Invero, l'art. 266 c.p.p. disciplina le «intercettazioni tra presenti» senza alcun riferimento espresso all'ambiente che, anzi, assume precipuo rilievo nel secondo periodo dell'ultimo comma del medesimo articolo, a mente del quale le intercettazioni in un luogo di privata dimora (*ex* art. 614 c.p.) sono consentite solo se ivi si stia svolgendo l'attività criminosa.

Secondo le Sezioni Unite, quindi, il punto di partenza per stabilire la necessarietà o meno dell'indicazione dei luoghi di privata dimora nel corpo del decreto autorizzativo risiedeva nella *summa divisio* tra intercettazioni tra presenti e intercettazioni tra presenti

---

L'intercettazione di comunicazioni, Cacucci, Bari, 2018, pp. 72 ss.

[45] Cass., Sez. VI, 26 giugno 2015, n. 27100, Musumeci, op. cit., p. 3.

[46] In particolare, secondo la sentenza Musumeci la specificazione dei luoghi in cui svolgere l'intercettazione virale non costituirebbe una mera «modalità attuativa» del mezzo di ricerca della prova, bensì una vera e propria «tecnica di captazione».

[47] Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, op. cit., §1.

[48] F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., p. 359.

[49] Ci si riferisce: (1) al d.l. 18 febbraio 2015, n. 7, recante «misure urgenti per il contrasto del terrorismo, anche di matrice internazionale», convertito con modificazioni dalla l. 17 aprile 2015, n. 43, con il quale era stato proposto di inserire un nuovo periodo all'interno dell'art. 266 *bis* c.p. («anche attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico»), successivamente espunto in sede di conversione; (2) alla proposta di legge del 02 dicembre 2015 C. 3470 intitolata «modifica all'art. 266 *bis* c.p.p., in materia di intercettazioni e di comunicazioni informatiche o telematiche»; (3) alla proposta di legge 20 aprile 2016 C. 3762.

nei luoghi di privata dimora: le prime non necessiterebbero di alcuna indicazione del luogo in cui essere svolte, dal momento che né l'art. 266 c.p.p., né la giurisprudenza della CEDU paiono orientarsi in tal senso[50]; mentre le seconde sarebbero ammissibili solo se vi è il fondato motivo di ritenere che all'interno del domicilio si stia perpetrando un crimine, ovvero in presenza della disciplina derogatoria prevista dall'art. 13 della l. 23 luglio 1991, n. 203[51].

Tale ultima disciplina, introdotta per garantire una maggiore efficacia dell'attività investigativa in un terreno delicato quale è quello del crimine organizzato, prevede che «quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo a un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa». In altre parole, se il delitto per il quale si procede concerne delitti di criminalità organizzata, il *fumus perdurantis criminis* non è un requisito essenziale del decreto autorizzativo.

A fortiori, poi, la Cassazione pone in evidenza come l'indicazione specifica dei luoghi sia sempre risultata superflua nei delitti di criminalità organizzata, utile solamente a fini pratici per consentire agli organi di PG di installare la cimice fisica. Non così, invece, per i restanti reati che seguono la disciplina ordinaria, relativamente ai quali l'indicazione della tipologia di ambienti è *conditio sine qua non* della legittimità delle operazioni investigative di intercettazione tra presenti in un luogo di privata dimora[52].

Tuttavia, vi è un elemento di difficoltà ulteriore per ciò che concerne l'intercettazione itinerante. Le "normali" intercettazioni ambientali, infatti, postulano che la captazione avvenga in un preciso luogo, quello in cui viene posizionata la microspia; l'intercettazione virale itinerante effettuata tramite l'infezione di un dispositivo elettronico portatile, al contrario, non presuppone uno specifico luogo in cui essere effettuata, bensì è identificata dal tipo di strumento sul quale il *trojan horse* viene

---

[50] «La necessità di uno specifico luogo – quale condizione di legittimità dell'intercettazione – non risulta inserita né nell'art. 266, comma 2 (in cui, con riferimento all'intercettazione di comunicazioni tra presenti, vi è solo la previsione di una specifica condizione per la legittimità dell'intercettazione se effettuata in un luogo di privata dimora), né nella giurisprudenza della Corte EDU secondo cui le garanzie minime che la legge nazionale deve apprestare nella materia delle intercettazioni riguardano la predeterminazione della tipologia delle comunicazioni oggetto di intercettazione, la ricognizione dei reati che giustificano tale mezzi di intrusione nella *privacy*, l'attribuzione a un organo indipendente dalla competenza ad autorizzare le intercettazioni con la previsione del controllo del giudice, la definizione delle categorie di persone che possono essere interessate, i limiti di durata delle intercettazioni, la procedura da osservare per l'esame, l'utilizzazione e la conservazione dei risultati ottenuti, la individuazione dei casi in cui le registrazioni devono essere distrutte» (Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, op. cit., §5).

[51] Ritiene che «due sono dunque i punti costituzionalmente scabrosi della pronuncia» C. PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di Stato"*, in questa *Rivista*, fasc. 4/2017, p. 80. Secondo l'Autore, la disciplina derogatoria prevista dall'art. 13 d.l. 152/1991 offre «un aggancio normativo sufficientemente solido», tuttavia le ingerenze nella sfera intima del soggetto, con l'utilizzo del virus di Stato, sono ben maggiori rispetto a un'intercettazione "classica" tra presenti. Inoltre, vi sarebbe in ogni caso un problema di compatibilità costituzionale dell'interpretazione giurisprudenziale con il principio della riserva di legge.

[52] V. *ex multis* Cass., Sez. I, 25 febbraio 2009, n. 11506, Molè; Cass., Sez. II, 08 aprile 2014, n. 17894, Alvaro.

installato. Per questo motivo la Suprema Corte è giunta a sostenere che le caratteristiche tecniche dell'intercettazione mediante virus informatico prescindono dal riferimento al luogo, trattandosi di un'intercettazione ambientale "itinerante", e perciò solo ontologicamente incompatibile con l'indicazione del luogo, non potendosi imporre agli organi di PG la disattivazione della captazione nel momento in cui il soggetto entra in un luogo di privata dimora. Ne consegue che, secondo il Supremo Collegio, al di fuori della disciplina derogatoria prevista per i delitti di criminalità organizzata (non essendo possibile prevedere in anticipo i luoghi in cui la captazione sarà effettuata) l'intercettazione itinerante dovuta all'inoculazione di un virus su di un dispositivo elettronico portatile non sarebbe ammissibile[53].

In altre parole, in assenza di una disciplina specifica sul tema, le Sezioni Unite Scurato erano giunte a sostenere, limitatamente alla potenzialità intercettiva itinerante, la legittimità di tale strumento di ricerca della prova tipico (art. 266 c.p.p.) attuato con "mezzi atipici avanguardistici" (il captatore informatico), ritenendola tuttavia ammissibile esclusivamente nel caso in cui si procedesse per delitti di criminalità organizzata – a cui si applica la disciplina derogatoria di cui all'art. 13 d.l. 152/1991 – definiti come qualsiasi reato associativo ascrivibile al protocollo di tipicità oggettiva dell'art. 416 c.p.[54]

4. La neo-introdotta disciplina legislativa del captatore informatico: il decreto legislativo 29 dicembre 2017, n. 216[55].

Con il d.lgs. 29 dicembre 2017, n. 216 – pubblicato in Gazzetta Ufficiale 11 gennaio 2018, n. 8 – il Governo ha dato seguito alla delega legislativa attribuitagli dall'art. 1,

---

[53] Per dirla con le parole delle Sezioni Unite: «muovendo da tali premesse e volendo giungere ad un primo approdo ermeneutico, deve escludersi – *de iure condito* – la possibilità di intercettazioni nei luoghi indicati dall'art. 614 c.p., con il mezzo del captatore informatico, al di fuori della disciplina derogatoria di cui alla L. n. 203 del 1991, art. 13» (Cass., Sez. Un., 01 luglio 2016, n. 26889, op. cit., §6).

[54] Sul tema si era acceso un nutrito dibattito in dottrina. V., *ex multis*, A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 5, 2016, pag. 2274; F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen.*, 11, 2016, p. 4140; A. CAPONE, *Intercettazioni e costituzione. Problemi vecchi e nuovi*, in *Cass. pen.*, 3, 2017, pp. 1263 ss.; A. GAITO – S. FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. Pen.*, 2, 2016, pp. 309 ss.; L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in questa *Rivista*, fasc. 3/2017, p. 177 ss.; G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in questa *Rivista*, 7 ottobre 2016; E. LORENZETTO, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, in questa *Rivista*, 24 marzo 2016; W. NOCERINO, *Le sezioni unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale*, in *Cass. pen.*, 10, 2016, pp. 3565 ss.; C. PARODI, *Intercettazioni telematiche e captatore, quali limiti?*, in *www.ilpenalista.it*, 06 novembre 2017; C. PELOSO, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *Dir. pen. cont. – Riv. trim.*, 1/2017, p. 149 ss.; C. PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite "virus di stato"*, op. cit., p. 75 ss.

[55] Forniscono una ricostruzione dettagliata dello stato dell'arte a seguito della novella: T. BENE (a cura di), *L'intercettazione di comunicazioni*, Cacucci, Bari, 2018; nonché S. SIGNORATO, *Le indagini digitali. Profili*

comma 84, l. 23 giugno 2017, n. 103[56] per riformare il delicato tema delle intercettazioni, i cui criteri direttivi, almeno secondo parte della dottrina, sono così dettagliati «da far pensare ad una veste normativa pressoché definitiva»[57].

Il *Leitmotiv* che permea la *ratio* riformatrice è posto nella tutela della riservatezza dei soggetti solo occasionalmente coinvolti dallo strumento captativo e, come tale, almeno secondo la relazione di accomunamento del decreto, l'intera novella dovrebbe essere interpretata alla luce della predetta garanzia a tutela della *privacy*[58]. Tuttavia il «modesto ritocco»[59] apportato dal legislatore delegato, nonostante gli originali propositi, ha finito per «scontentare tutti»[60], dal momento che non ha garantito il diritto di difesa né dell'imputato né della persona offesa dal reato.

Per quanto qui di interesse, la novella volta a disciplinare e a circoscrivere l'ambito applicativo del *Trojan horse* è lacunosa, essendo limitata sia dal punto di vista delle potenzialità intrusive del captatore informatico, sia da quello del dispositivo infettabile: il parlamento, infatti, si è preoccupato di delegare il governo assumendo quale punto di riferimento esclusivamente i principi dettati dalla sentenza Scurato pronunciata dalla Suprema Corte nel suo massimo consesso[61]. Una riforma, quindi, da questo punto di vista, anacronistica *ab origine*[62]. Tale affermazione è peraltro suggellata

---

strutturali di una metamorfosi investigativa, Giappichelli, Torino, 2018.

[56] Parte della dottrina pone in evidenza come un precursore della attuale disciplina possa rinvenirsi nei lavori parlamentari già in un momento temporale concomitante con la pronuncia delle Sezioni Unite Scurato, sottolineandone le analogie e le differenze. Sul punto v. F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., pp. 354 ss. Per i primi commenti alla delega Orlando in tema di intercettazioni v. anche A. CAMON, *Intercettazioni e fughe di notizie: dal sistema delle circolari alla riforma Orlando*, in *Arch. pen*., 2, 2017, pp. 1 ss; C. CONTI, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *Dir. pen. cont. – Riv. trim.*, 3/2017, pp. 79 ss.; M. GIANLUZ, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazioni della giurisprudenza, riforme attese da tempo e confuse innovazioni*, *ivi*, 3/2017, pp. 173 ss.

[57] D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 383.

[58] «Dette disposizioni perseguono lo scopo di escludere, in tempi ragionevolmente certi e prossimi alla conclusione delle indagini, ogni riferimento a persone solo occasionalmente coinvolte dall'attività di ascolto e di espungere il materiale documentale, ivi compreso quello registrato, non rilevante a fini di giustizia, nella prospettiva di impedire l'indebita divulgazione di fatti e riferimento a persone estranee alla vicenda oggetto dell'attività investigativa che ha giustificato il ricorso a tale incisivo mezzo di ricerca della prova» (C.D.M., *D.lgs. – Disposizioni in materia di intercettazione di conversazioni o comunicazioni, in attuazione dell'art. 1, legge 23 giugno 2017, n. 103 – Relazione*, in *www.giurisprudenzapenale.it*).

[59] L. FILIPPI, *Pubblicata in gazzetta la riforma delle intercettazioni*, in *www.pluris-cedam.utetgiuridica.it*, 12 gennaio 2018, p. 7.

[60] L. FILIPPI, *Pubblicata in gazzetta*, op. cit., p. 1.

[61] Cass., Sez. Un., 1 luglio 2016, n. 26889, Scurato, op. cit. Con il riferimento esclusivo alle Sezioni Unite Scurato si sono avverati i timori di parte della dottrina sul tema generale delle indagini informatiche. A causa della tecnica di redazione legislativa imperfetta, invero, si andrebbe incontro a un duplice rischio: «da un lato, quello di legiferare in base ad una concezione di fondo tipica del mondo della rete che tende a prediligere un approccio intuitivo ed emotivo ad uno analitico sistematico. Dall'altro, il rischio che la molteplicità dei problemi che emergono nella prassi applicativa porti il legislatore a risolvere i problemi concreti con un pragmatismo disancorato dai principi», con la conseguenza di «sospingersi nella direzione di un modo di operare caratterizzato dalla precarietà e dalla destrutturazione» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 47).

[62] Così anche D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 389, secondo cui il limite principale della delega e, di conseguenza, del decreto delegato consiste nell'aver «ristretto l'uso del

da alcune recenti dichiarazioni del Ministro Guardasigilli circa la volontà di voler rivedere la riforma Orlando sul tema delle intercettazioni, a cui ha fatto seguito, nel decreto milleproroghe 2018, la postergazione del termine di entrata in vigore della disciplina di cui al d.lgs. 216/2017 al 31 marzo 2019[63].

4.1. La funzione di intercettazione ambientale.

Come si è avuto modo di notare in precedenza, la funzionalità poliedrica del virus di Stato può consentire un controllo "orwelliano" della vita di ogni singolo soggetto. Per tale motivo il legislatore delegante, stante la delicatezza del tema, ha tentato di farsi carico del problema, basando purtroppo l'orizzonte conoscitivo delle potenzialità del mezzo in questione limitatamente a quanto prescritto dalla sentenza Scurato, circoscrivendo di conseguenza l'intervento riformatore esclusivamente alle funzioni di intercettazione ambientale itinerante[64]. L'art. 1, comma 84, lett. *e*, l. 103/2017, infatti, delega il Governo a «disciplinare le *intercettazioni* di comunicazioni o conversazioni *tra presenti* mediante l'immissione di captatore informatici in *dispostivi elettronici portatili*», prevedendo altresì che l'«attivazione del *microfono*» avvenga solo in seguito ad apposito comando.

Il Governo, nella veste di legislatore delegato, ha così dovuto confrontarsi con una delega insoddisfacente e vi ha dato seguito con l'art. 4 d.lgs. 216/2017, rubricato «modifiche al codice di procedura penale in materia di intercettazioni mediante inserimento di captatore informatico».

La novella in oggetto ha introdotto un nuovo periodo all'art. 266, comma 2, c.p.p. in virtù del quale è oggi possibile procedere all'intercettazione di comunicazioni tra presenti «*anche* mediante l'inserimento di un captatore informatico su un dispositivo

captatore alla sola attività di intercettazione tra presenti attraverso l'attivazione del microfono». Dello stesso avviso M. TORRE, *Il captatore informatico nella legge delega 23 giugno 2017, n. 103*, in *Jusonline*, 3, 2017, p. 437: «il vero problema -del quale il legislatore non si è fatto carico- consiste nella poliedricità del captatore informatico».

[63] L'art. 2 d.l. 25 luglio 2018, n. 91, ha infatti modificato l'art. 9, comma 1, d.lgs. 216/2017 nei termini che seguono: «le disposizioni di cui agli articoli 2, 3 4, 5 e 7 si applicano alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019».

[64] Di tale "lacuna" nella delega è ben conscio il Governo: «come si ricava dal chiaro tenore della delega e dai sopramenzionati criteri per la sua attuazione, il delegante ha inteso regolamentare uno solo degli usi del captatore informatico, quale modalità specifica di esecuzione delle intercettazioni tra presenti, ed ha ad oggetto esclusivamente dispositivi mobili portatili» (C.D.M., *D.lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 9). Vi è poi chi, anche in dottrina, sostiene che «probabilmente i tempi non sono ancora maturi per un'organica disciplina di tutte le attività che possono essere svolti dal captatore informatico» (F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., p. 357).

elettronico portatile»[65-66]. Come agevolmente si può intuire anche dalla collocazione sistematica delle disposizioni in esame[67], il legislatore ha sopito il dibattito dottrinale e giurisprudenziale che era sorto in relazione alla sussunzione dell'intercettazione itinerante nel più ampio *genus* delle intercettazioni tra presenti: la presa di posizione si è dunque allineata, da questo punto di vista, al *dictum* delle Sezioni Unite Scurato[68].

Da quest'ultima decisione, tuttavia, il legislatore – «evidentemente incerto»[69] – si discosta notevolmente quanto ai delitti in ordine ai quali l'intercettazione virale è ammissibile. Le Sezioni Unite, infatti, avevano "circoscritto diffusamente" l'orizzonte applicativo del captatore informatico: "circoscritto" nel momento in cui avevano ritenuto legittimo un tale innovativo strumento di ricerca della prova per i soli delitti di criminalità organizzata; "diffusamente" perché la nozione di criminalità organizzata era tale da ricomprendere ogni delitto sussumibile nel modulo di incriminazione di cui all'art. 416 c.p.[70]. Il legislatore, non modificando in alcun modo l'art. 266, comma 1, c.p.p. – che racchiude l'elencazione dei delitti in ordine ai quali è possibile procedere con il mezzo di ricerca della prova "tradizionale" – e non specificando alcuna deroga nel comma 2 del medesimo articolo, ha ritenuto preferibile estendere il catalogo di reati per i quali è possibile procedere alla captazione itinerante, allargando così in modo non

---

[65] In dottrina, diversamente da quanto disposto dal legislatore delegato, sia era ipotizzato o di introdurre *ex novo* un art. 266 *ter* c.p.p., dedicato esclusivamente alla funzione di intercettazione virale di comunicazioni o conversazioni tra presenti (così D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 383 e F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., p. 367), ovvero un nuovo comma 2 *bis* all'art. 266 c.p.p. (D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 383).

[66] Non condivide la scelta del legislatore D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 383, dal momento che «la previsione avrebbe bisogno di un'autonoma comma, se non addirittura di un'autonoma norma, vista la mole di problemi giuridici, tecnici ed ermeneutici che questa nuova forma di intercettazione porrà agli operatori del diritto».

[67] Critica riguardo alla scelta del legislatore di intervenire sull'art. 266 c.p.p. anziché sull'art. 266 *bis* c.p.p. S. SIGNORATO, *Le indagini digitali*, op. cit., p. 242. L'Autore ritiene che la funzione di intercettazione itinerante si confarebbe maggiormente alla disciplina delle intercettazioni telematiche di cui all'art. 266 *bis* c.p.p., nonostante la stessa ritenga comunque che non vi sarebbe più motivo per mantenere una obsoleta distinzione tra intercettazioni telefoniche e intercettazioni telematiche. Inoltre, puntualizza come la scelta di fondo del legislatore sarebbe «contraddetta dalla stessa riforma», atteso che «nel disciplinare le tipologie di impianti con i quali l'intercettazione tramite *trojan* deve essere effettuata, il legislatore inserisce infatti una novella in materia non già all'art. 268, comma 3 c.p.p., che si riferisce alle intercettazioni ordinarie, ma all'art. 268, comma 3-*bis* c.p.p. specificamente dettato per le intercettazioni di comunicazioni informatiche e telematiche» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 242).

[68] Critica la riconduzione alla disciplina delle intercettazioni tra presenti F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., p. 360, dal momento che non sarebbe «indice di particolare sforzi di riflessione da parte del legislatore». Così anche D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 395: «nell'ottica riformista, il *virus* dovrebbe essere paragonato, *tout court*, alle tradizionali microspie».

[69] M. GRIFFO, *Una proposta costituzionalmente orientata*, op. cit., p. 40.

[70] «Per reati di criminalità organizzata devono intendersi non solo quelli elencati nell'art. 51 c.p.p., commi 3-*bis* e 3-*quater*, ma anche quelli comunque facenti capo a un'associazione per delinquere, *ex* art. 416 c.p., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato» (Cass., Sez. Un., 1 luglio 2016, n. 26889, Scurato, op. cit. §16).

indifferente l'ambito applicativo dell'istituto in esame rispetto al "regime pretorio" previgente[71].

Il legislatore si discosta dalla decisione del Supremo Collegio anche in relazione alla possibilità di effettuare intercettazioni «ubiquitarie»[72] in un luogo di privata dimora, al di fuori della disciplina derogatoria per i delitti di criminalità organizzata di cui all'art. 13 d.l. 152/1991. Invero, secondo la Cassazione non sarebbe stato possibile per il giudice delle indagini preliminari prevedere in anticipo i luoghi di privata dimora in cui il dispositivo elettronico portatile sarebbe andato a trovarsi e, di conseguenza, indicarli nel decreto autorizzativo[73]; del pari non era immaginabile per gli operanti di P.G. seguire gli spostamenti del bersaglio e disattivare la captazione al momento dell'ingresso in un luogo di privata dimora[74]. Il legislatore, al contrario, effettua una scelta diametralmente opposta a quella a cui era pervenuta la Nomofilachia, dal momento che ritiene ammissibile la captazione virale-itinerante-domiciliare nel caso in cui vi sia il fondato motivo di ritenere che in un luogo di privata dimora si stia svolgendo l'attività criminosa[75]. L'art. 266, comma 2, secondo periodo, c.p.p. non ha subito infatti alcuna variazione ed è posto in continuità con il precedente periodo che ammette l'intercettazione captativa[76].

---

[71] In altre parole, «evidente, dunque, l'asimmetria tra ambito di ammissibilità che appaiono come cerchi intersecanti: da un lato, la scelta legislativa di restringere in numero di reati per l'accertamento dei quali è consentito il ricorso al captatore informatico […]; dall'altro lato, tuttavia, il legislatore delegante fa rientrare dalla finestra ciò che le sezioni unite sembravano aver fatto uscire dalla porta principale, ossia la possibilità di impiegare il captatore informatico quando si procede per reati "comuni"» (M. TORRE, *Il captatore informatico nella legge delega 23 giugno 2017, n. 103*, op. cit., p. 438).

[72] Parla di intercettazioni ubiquitarie G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2016, p. 88.

[73] Per dirla con le parole della Cassazione: «all'atto di autorizzare una intercettazione da effettuarsi a mezzo di captatore informatico installato su di un apparecchio portatile, il giudice non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico […] verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale» (Cass., Sez. Un., 1 luglio 2016, n. 26889, Scurato, op. cit. §6).

[74] Tale ragionamento può ricavarsi da un'argomentazione *ad absurdum* della stessa Corte di Cassazione: «peraltro, anche se fosse teoricamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione nel caso di ingresso in un luogo di privata dimora, sarebbe comunque impedito il controllo del giudice al momento dell'autorizzazione, che verrebbe disposta "al buio"» (Cass., Sez. Un., 1 luglio 2016, n. 26889, Scurato, op. cit. §6).

[75] Precisa T. ALESCI, *Le intrusioni* inter praesentes, op. cit., p. 77 che «il fondato motivo di ritenere non postula che detta attività debba essere stata effettivamente sussistente, dovendosi considerare sufficiente, sulla base del dato normativo […], che dell'attività in questione possa, con giudizio *ex ante* ragionevolmente ritenersi la sussistenza dell'emanazione del provvedimento di autorizzazione all'effettuazione delle operazioni».

[76] Per semplicità espositiva si riporta il novellato art. 266, comma 2, c.p.p.: «negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

La possibilità di procedere alla avanguardistica intercettazione nei luoghi di cui all'art. 614 c.p. è poi confermata indirettamente dall'art. 266, comma 2 *bis*, c.p.p. – a mente del quale è sempre consentita l'intercettazione virale domiciliare se si procede per i delitti elencati nell'art. 51, commi 3 *bis* e 3 *quater*, c.p.p. – e dal rafforzato onere motivazionale imposto al giudice per le indagini preliminari dall'art. 267, comma 1, ult. per., c.p.p. Il gip, infatti, deve indicare nel provvedimento autorizzativo «i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono».

In assenza di pronunce giurisprudenziali sul punto, la dottrina[77] si è chiesta quale debba essere il livello di precisione richiesto al gip per l'indicazione, anche indiretta, dei luoghi e del tempo. Il legislatore delegato era ben consapevole della difficoltà di prevedere nel dettaglio gli spostamenti di un dispositivo portatile e, di conseguenza, di indicare nel decreto autorizzativo i tempi e i luoghi in cui attivare il microfono per la captazione audiofonica[78]: proprio per tale motivo ci si deve domandare quale sia il livello massimo di indeterminatezza concesso al giudice nel proprio decreto, dal momento che una indicazione eccessivamente meticolosa rischia di rendere inutile lo strumento investigativo, mentre l'indeterminatezza totale del decreto renderebbe la tecnica captativa *ad explorandum* e dunque inutilizzabile.

Il luogo è uno dei due requisiti richiesti nel decreto giudiziale. La novità della previsione traccia una linea di cesura con quanto sancito dalle Sezioni Unite Scurato: queste ultime, infatti, ritenevano che l'indicazione del luogo fosse una mera modalità attuativa, volta a fornire indicazioni per l'esecuzione dell'intercettazione[79]. Al contrario, il legislatore ha ritenuto preferibile annoverare l'indicazione del luogo – insieme a quella del tempo – tra i presupposti del provvedimento autorizzativo (art. 267, comma 1, c.p.p.), i quali sono garantiti da una espressa comminatoria di inutilizzabilità del risultato intercettivo (art. 271, comma 1, c.p.p.)[80]: il tutto al verosimile fine di garantire

---

[77] C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n. 216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria*, in questa *Rivista*, 13 aprile 2018, pp. 24 s.; M. GRIFFO, *Una proposta costituzionalmente orientata*, op. cit., p. 40; D. PRETTI, *Prime riflessioni a margine*, op. cit., pp. 219 ss.

[78] Si legge, infatti, nella relazione di accompagnamento al d.lgs. 216/2017 che «la formula – secondo la quale nel decreto autorizzativo i luoghi e il tempo, in cui il dispositivo può essere attivato da remoto, possono essere "anche indirettamente determinati" – si spiega, dunque, nell'impossibilità di prevedere specificamente tutti gli spostamenti dell'apparecchio controllato; da qui la necessità logica di delimitare gli ambiti ai verosimili spostamenti del soggetto, in base alle emergenze investigative. A titolo esemplificativo, valga il riferimento a formule del tipo: "ovunque incontri il soggetto x"; "ogni volta che si rechi nel locale y" ecc. ecc.» (C.D.M., *D.lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 10). Anche la dottrina sul punto ha evidenziato «l'impossibilità di predeterminare con certezza gli spostamenti del supporto informatico sul quale insiste il *trojan horse*» (T. ALESCI, *Le intrusioni* inter praesentes, op. cit., p. 78).

[79] «La tesi sostenuta nella sentenza n. 27100/15 in ordine alla necessità di individuare con precisione, a pena di inutilizzabilità, i "luoghi" nei quali le intercettazioni tra presenti devono essere espletate, si pone altresì in palese difformità rispetto alla consolidata giurisprudenza che ha sempre escluso la necessità di una tale indicazione, ad eccezione dei luoghi di privata dimora, per i quali vale il disposto dell'art. 266 c.p.p., comma 2» (Cass., Sez. Un., 1 luglio 2016, n. 26889, Scurato, op. cit. §8).

[80] Nel previgente regime, dal momento che l'indicazione del tempo e del luogo non erano espressamente annoverati tra i presupposti del provvedimento, la sanzione dell'inutilizzabilità non era comminabile. Il

un bilanciamento tra le esigenze investigative e quelle private, garantendo un controllo successivo da parte del soggetto destinatario ignaro della captazione.

In ogni caso, stante la materiale difficoltà di determinare a priori il luogo in cui la captazione verrà effettuata, sarà sufficiente rimandare ad accadimenti della vita quotidiana strettamente connessi con il delitto per il quale si procede, nella speranza che la giurisprudenza «non si mostri eccessivamente rigida nello scrutinio a posteriori della sufficiente determinatezza dei provvedimenti autorizzativi»[81]. In dottrina[82] si è portato l'esempio della lotta allo spaccio di sostanze psicotrope o stupefacenti. Si ponga il caso che la Procura venga a conoscenza – magari per mezzo di un informatore o di una intercettazione telefonica – che Tizio, noto spacciatore contro il quale si procede, debba incontrarsi con Caio per la cessione di un ingente quantitativo di sostanza, ma non si sia a conoscenza dell'ubicazione del luogo dello scambio. In tal caso il provvedimento autorizzativo dell'intercettazione itinerante potrebbe rimandare indirettamente al luogo dello scambio, con una formula ampia quale "nel luogo in cui Tizio incontrerà Caio per cedergli la sostanza stupefacente". Non vi sarebbe alcun problema anche nel caso in cui il luogo di consumazione del reato (nel caso di specie la cessione) fosse domiciliare, dal momento in una simile situazione si svolge l'attività criminosa all'interno di un luogo di cui all'art. 614 c.p.; quindi, ancor prima, al momento dell'autorizzazione, vi era il fondato motivo di ritenere che all'interno di un luogo di privata dimora si potesse svolgere un'attività criminosa.

Tuttavia, quanto appena affermato può avere valenza meramente esemplificatoria. Invero, pare decisamente arduo (se non addirittura impossibile) valutare in astratto il livello di determinatezza dell'indicazione del luogo, poiché ogni fatto storico necessita del proprio specifico approfondimento. Si può immaginare che la giurisprudenza utilizzerà formule generali ampie per valutare la precisione della delimitazione spaziale, le quali tuttavia di per sé non possono assumere un significato precettivo se non calate nell'orizzonte specifico della fattispecie concreta[83].

Simili problematiche paiono essere superabili, almeno secondo parte della dottrina[84], ove si accogliesse una accezione estesa di domicilio, idonea ad abbracciare anche il domicilio informatico[85]. Così ragionando, infatti, il luogo di privata dimora nel

---

rimando operato dall'art. 271 c.p.p. all'art. 267 c.p.p. deve oggi considerarsi esteso interamente a questo ultimo articolo. Sul punto v. anche C. GITTARDI, *Linee guida*, op. cit., p. 30.

[81] D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 220.

[82] C. GITTARDI, *Linee guida*, op. cit., p. 24; D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 221.

[83] Si pensi che vi sono già nel panorama giurisprudenziale affermazioni di principio che assumono significato esclusivamente se calate nel panorama applicativo. A mero titolo esemplificativo si pensi alla definizione di atto abnorme quale «provvedimento caratterizzato dall'esercizio di un potere totalmente avulso dal sistema che determina la stasi del procedimento e che legittima quindi il ricorso per Cassazione al di fuori del principio di tassatività delle impugnazioni di cui all'art. 568 cod. proc. pen.» (Cass., Sez. Un., 26 marzo 2009, n. 25957, Toni, in *CED* n. Rv 24359): è indubbio che vi sia una definizione, la quale però deve essere raffrontata ogni singola volta al caso di specie.

[84] S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 244 ss.

[85] Per un approfondimento sulla nozione di domicilio informatico v. *ex multis* R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di «domicilio informatico» e lo* jus excludendi alios, in *Dir. pen. proc.*, 2005, pp. 81 ss; R. FLOR, *Lotta alla «criminalità informatica» e tutela di «tradizionali» e «nuovi» diritti fondamentali*

quale viene effettuata l'intercettazione itinerante non si rinverrebbe nello spazio fisico nel quale è presente il dispositivo elettronico portatile infettato, bensì nello *smartphone* stesso. In altre parole, il captatore è la cimice, mentre il domicilio è lo *smartphone*, a condizione che quest'ultimo soddisfi «i requisiti dello *ius includendi se*; dello *ius includendi et excludendi alios* e della destinazione del luogo ad attività private tipiche della vita domestica o a spazio di attività lavorativa»[86].

Come corollario di tale lettura, il fondato motivo di ritenere che si stia svolgendo l'attività criminosa dovrebbe essere riferito al dispositivo elettronico portatile infetto, e non al luogo fisico in cui avviene l'intercettazione, rimanendo così «del tutto residuale»[87] l'ipotesi di intercettazione itinerante al di fuori di un luogo di cui all'art. 614 c.p.

Infine, se si seguisse la suddetta lettura sarebbe necessario domandarsi quale valore semantico attribuire alla nozione di indicazione di luoghi "indirettamente determinati" di cui all'art. 267, comma 1, c.p.p. *Prima facie* potrebbe sostenersi che i luoghi sarebbero sempre determinati, poiché non si comprende come il dispositivo bersaglio possa essere indicato indirettamente. Tuttavia, il dispositivo bersaglio in uso a un soggetto determinato potrebbe non essere sempre il medesimo: l'utenza (*rectius*: lo *smartphone*) oggetto di intercettazione potrebbe essere ceduta dal proprietario a un terzo; ovvero potrebbe accadere che il dispositivo *target* presenti dei malfunzionamenti o diventi inutilizzabile per i più vari motivi e, quindi, venga sostituito l'organismo ospite. L'indicazione dei luoghi in modo indiretto, quindi, potrebbe riassumersi in formule generiche del tipo «il dispositivo mobile appartenente a Tizio», non specificando la marca e il numero seriale dello stesso, così consentendo l'intercettazione itinerante anche nel caso di successione nel tempo di dispositivi mobili.

In ogni caso, un elemento di totale novità è dato dalla necessaria indicazione del tempo di attivazione del microfono già nel provvedimento autorizzativo dell'intercettazione itinerante, il quale si affianca – e non si sostituisce – alla durata delle intercettazioni disposte[88]. In tal modo si crea una netta differenza tra le intercettazioni tradizionali, le quali proseguono ininterrottamente per tutto l'arco temporale in cui sono autorizzate (normalmente 15 giorni ed eventuali successive proroghe), e quelle itineranti, i cui momenti temporali di attivazione necessitano di un apposito comando

---

nell'era di internet, in questa *Rivista*, 20 settembre 2012; R.E. KOSTORIS, *La costruzione dei diritti fondamentali, la Carta di Nizza e le prospettive di adesione dell'Unione alla Cedu*, in R.E. Kostoris, (a cura di), *Manuale di procedura penale europea*, III ed., Giuffrè, Milano, 2017; S. SIGNORATO, *Le indagini digitali*, op. cit., pp. 49 ss.; A. PAPA, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Giappichelli, Torino, 2009; V. ZAGREBELSKY – R. CHENALE – L. TOMASI, *Manuale dei diritti fondamentali in Europa*, Il Mulino, Bologna, 2016.

[86] S. SIGNORATO, *Le indagini digitali*, op. cit., p. 246.

[87] S. SIGNORATO, *Le indagini digitali*, op. cit., p. 246.

[88] L'indicazione delle coordinate temporale costituisce un elemento di novità significativa, dal momento che le «limitazioni spaziali costituivano già, a seconda dei casi, patrimonio della disciplina delle intercettazioni» (D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 221).

dell'autorità giudiziaria procedente[89], i quali comunque devono rimanere confinati nel perimetro di durata massima dell'intercettazione[90].

Anche in questo caso il giudice per le indagini preliminari potrà ricorrere a una indicazione «indirettamente determinata» del tempo in cui si potrà procedere all'intercettazione virale-ambientale, a condizione comunque che non autorizzi una captazione *ad explorandum*[91]: anche in questo caso non sembrano potersi definire a priori e in linea teorico-astratta – così come evidenziato sul tema dell'indicazione spaziale – criteri direttivi avulsi da ogni fattispecie concreta.

In ogni caso, l'indicazione spaziale, unita a quella temporale, dovrebbe consentire di non dilatare eccessivamente l'ambito applicativo dell'istituto in esame, sebbene permanga la possibilità che elementi utili alle indagini possano presentarsi in un momento in cui la captazione itinerante non è autorizzata.

Le considerazioni appena svolte, tuttavia, non trovano applicazione ai casi in cui si proceda per un grave delitto di criminalità organizzata o terroristica elencato nell'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., ai quali si applica la disciplina derogatoria di cui all'art.

---

[89] Non bisogna dimenticare che se il virus informatico agisse indisturbato per tutto l'arco della giornata, il dispositivo captato andrebbe incontro a un repentino consumo di batteria e a un ingente consumo di traffico dati, così mettendo a rischio la copertura investigativa. Sul punto v. E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in AA. VV., Trojan horse*: tecnologia, indagini e garanzie di libertà (profili di* intelligence*)*, in *www.parolaalladifesa.it*, 06 settembre 2016, p. 161; M. ZONARO, *Aspetti tecnici e operativi*, op. cit., p. 166. Al contrario, secondo D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 400, sarebbero proprio le operazioni di attivazione e disattivazione del microfono la causa principale di esaurimento precoce della carica della batteria del dispositivo portatile.

[90] Esemplificando, l'attività di intercettazione "tradizionale" è autorizzata dal 10/10/2018 al 25/10/2018. È in questo lasso temporale di 15 giorni che il giudice deve indicare i tempi in cui il microfono potrà essere attivato, procedendo così all'intercettazione itinerante.

[91] Per comprendere meglio un tale assunto, in dottrina si è portato il seguente esempio: «si pensi al procedimento a carico di due sodali individuati quali autori di una rapina; ottenuta l'autorizzazione all'attivazione degli ascolti mediante *trojan horse* inoculato sul dispositivo telefonico portatile di uno dei due indagati in vista dell'incontro tra i due, in area campestre, per la spartizione del profitto del reato, potrà accadere che i due interlocutori si accordino, in quella sede, anche in vista di un ulteriore "colpo" da mettere a segno in seguito, dandosi appuntamento per un nuovo incontro finalizzato alla predisposizione delle specifiche modalità operative del nuovo reato da perpetrare. In tal caso, è possibile che l'autorizzazione abbia legittimato l'intercettazione in occasione del primo incontro limitando ad esso, e ad esso solo, la facoltà di attivazione del microfono, ragione per cui il decreto del pubblico ministero che ha disposto le operazioni avrà recepito la durata complessiva limitatamente a quell'incontro, con la conseguenza che sarà necessaria una nuova autorizzazione ed un nuovo decreto in vista dell'incontro successivo. Al contrario, è possibile ipotizzare anche che il giudice abbia autorizzato, indirettamente, la captazione in ragione di ogni incontro che si svolgerà in quel luogo (o in altri luoghi) in vista di tutte le possibili occasioni d'incontro tra i due sodali: in tal caso, non sarà necessaria una nuova autorizzazione e l'ascolto avrà luogo, con attivazione del microfono ad intermittenza, ad ogni occasione d'incontro, per tutta la durata fissata con il decreto del pubblico ministero, di cui si potrà comunque disporre la proroga ad opera del giudice» (D. PRETTI, *Prime riflessioni a margine*, op. cit., pp. 221 s.).

13 d.l. 152/1991[92]. Invero, l'art. 266, comma 2 *bis*, c.p.p.[93] consente in ogni caso l'intercettazione itinerante, anche se avviene in un luogo di privata dimora, se si procede per uno dei gravi delitti testé citati, circoscrivendo così l'ambito applicativo che era stato in precedenza disegnato dalle Sezioni Unite Scurato. A detta di queste ultime, infatti, il riferimento ai delitti di criminalità organizzata non doveva ricondursi alle fattispecie delittuose di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., bensì doveva estendersi a qualsiasi delitto riconducibile al protocollo di tipicità oggettiva dell'art. 416 c.p.: da questo punto di vista il legislatore ha avuto il pregio di recepire quelle preoccupazioni che erano sorte in dottrina in merito a un potenziale uso eccessivo del captatore informatico[94].

Infine, un accenno è d'obbligo al c.d. "terzo binario"[95] processuale in tema di intercettazioni, i cui presupposti di applicabilità, in seguito alla riforma, sono rimasti sostanzialmente invariati, laddove, invece, si sono allargate le maglie per i delitti dei pubblici ufficiali contro la pubblica amministrazione[96].

Dispone infatti l'art. 6 d.lgs. 216/2017 che «nei procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 del codice di procedura penale, si applicano le disposizioni di cui all'art. 13 del decreto-legge 13

---

[92] Per tali delitti il compendio accusatorio *in fieri* non dovrà basarsi su «*gravi* indizi di reato» e su di una *assoluta* indispensabilità del mezzo di ricerca della prova ai fini della *prosecuzione* delle indagini (art. 267, comma 1, c.p.p.); ma i presupposti applicativi saranno soddisfatti da un quadro indiziario sufficiente («*sufficienti* indizi»), qualora l'intercettazione sia «*necessaria* ai fini dello *svolgimento* delle indagini (art. 13 d.l. 152/1991). Quindi, sufficienti e non gravi indizi di reato, necessarietà e non assoluta indispensabilità ai fini dello svolgimento (non per la prosecuzione) delle indagini. Inoltre, il lasso temporale di utilizzo dello strumento captativo subisce una netta rimodulazione, laddove la legislazione speciale consente di ricorrere alle intercettazioni di comunicazioni o conversazioni telefoniche e di altre forme di telecomunicazione per un periodo iniziale di 40 giorni, con successive proroghe di 20, a fronte dei 15 giorni, con relative proroghe di 15, prescritte dal codice di rito.

[93] Il comma in questione, che «amplia le coordinate del doppio binario» (T. ALESCI, *Le intrusioni* inter praesentes, op. cit., p. 79) è stato introdotto dall'art. 4 d.lgs. 29 dicembre 2017, n. 216.

[94] V. *ex multis* F. CAJANI, *Odissea del captatore informatico*, op. cit., pp. 4140 ss.; M. DI STEFANO, *Grande fratello sì, intercettazioni con lo smartphone ma solo per la criminalità organizzata*, in *Foro it.*, II, 2016, pp. 516 ss.; G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "fra presenti"*, op. cit.; M. TORRE, *Il captatore informatico*, op. cit., pp. 37 ss.

[95] Il terzo binario si affianca al primo, costituito dalla disciplina processuale ordinaria; e al secondo, costituito dalle deroghe disciplinate nell'art. 51 c.p.p.

[96] Secondo L. FILIPPI, *Pubblicata in gazzetta*, op. cit., p. 1 «la nuova disciplina non ridurrà di certo l'attuale eccessivo numero di intercettazioni», eccessivamente inflazionate – anche in virtù di interpretazioni estensive della giurisprudenza in relazione ai presupposti applicativi – e costose per il sistema. Al contrario, secondo il C.S.M. «va ribadito con decisione che il rimedio alla divulgazione non può essere rappresentato dalla riduzione dell'area operativa del mezzo di ricerca della prova in esame, che è indispensabile per le investigazioni (C.S.M., *Ricognizione di buone prassi in materia di intercettazioni di conversazioni*, in www.csm.it, 29 luglio 2016, p. 16).

maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203»[97-98-99]. Riassumendo, quindi, nei casi in cui si proceda per delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con pena non inferiore nel massimo a cinque anni, potranno effettuarsi:

1) intercettazioni telefoniche e ambientali – queste ultime al di fuori dai luoghi di privata dimora – qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini dello svolgimento delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20;
2) intercettazioni ambientali "tradizionali" nei luoghi di privata dimora, anche in assenza di un fondato motivo per ritenere che all'interno si stia svolgendo l'attività criminosa, qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini dello svolgimento delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20;

---

[97] L'art. 1, comma 84, lett. d, della legge delega 103/2017 imponeva, più genericamente, di «prevedere la semplificazione delle condizioni per l'impiego delle intercettazioni delle conversazioni e delle comunicazioni telefoniche e telematiche nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione».

[98] È d'uopo notare che traspare dalla relazione di accompagnamento al decreto legislativo una disattenzione di fondo nelle intenzioni del legislatore delegato, il quale utilizza come sinonimi le differenti locuzioni di "prosecuzione" e "svolgimento". Si legge, infatti, nella relazione citata che «si interviene, con autonoma disposizione, per consentire alle intercettazioni, nei casi già previsti dalla legge [...] sulla base dei presupposti dei sufficienti indizi di reato e della necessità per lo *svolgimento* delle indagini» (C.D.M., *D.lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 11). Un utilizzo promiscuo di terminologia dai contorni affatto differenti, che potrebbe condurre a divergenze esegetiche sul punto in sede di prima applicazione nelle sedi giudiziarie e non solo.

[99] Il rinvio, effettuato dall'art. 6 d.lgs. 216/2017, all'art. 13 d.l. 152/1991, impone altresì un'attenta analisi in ordine alla necessaria sussistenza di un *fumus perdurantis criminis* qualora l'intercettazione sia disposta nei luoghi di privata dimora *ex* art. 614 c.p. Il problema sorge dal momento che il primo periodo dell'art. 13 cit. prescrive una deroga all'ordinaria disciplina in tema di intercettazioni per i reati di criminalità organizzata e di minaccia col mezzo del telefono; mentre il secondo periodo statuisce che quando si tratta di intercettazione ambientale disposta in un procedimento relativo esclusivamente a un delitto di criminalità organizzata – non anche di minaccia col mezzo del telefono – l'intercettazione, in deroga all'ordinaria disciplina, è consentita anche se non vi è motivo di ritenere che nel domicilio si stia svolgendo l'attività criminosa. Ci si chiede, in altri termini, se il rinvio debba considerarsi esteso per intero all'art. 13 d.l. 152/1991, ovvero se, al contrario, l'ambito applicativo debba considerarsi circoscritto al solo primo periodo dell'articolo citato.

Pare fornire una soluzione al quesito il comma 3 dell'art. 6 d.lgs. 216/2017, a mente del quale «l'intercettazione di comunicazioni tra presenti nei luoghi indicati dall'art. 614 del codice penale non può essere eseguita mediante l'inserimento di un captatore informatico su dispositivo elettronico portatile quando non vi è motivo di ritenere che ivi si stia svolgendo l'attività criminosa». Ne deriva, *a contrario*, stante il tenore della norma, che qualora l'intercettazione ambientale sia disposta nel domicilio senza l'utilizzo del captatore informatico, essa sia legittima anche in assenza del *fumus perdurantis criminis*. È verosimile che una simile previsione sia dettata al chiaro scopo di uniformare la disciplina *de qua* con quella generale in tema di intercettazioni di comunicazioni e conversazioni tra presenti con lo strumento del captatore informatico. Il legislatore, infatti, con l'intervento riformatore ha previsto che, stante l'elevata intrusività nella sfera personale del soggetto coinvolto, l'intercettazione con virus *Trojan horse* sia espletabile all'interno del domicilio solo nel caso in cui si proceda per i più gravi delitti di criminalità organizzata, di stampo mafioso, eversiva o terroristica ai sensi dell'art, 51, commi 3 *bis* e 3 *quater*, c.p.p., riducendo così l'ambito applicativo originalmente tracciato con la sentenza Scurato delle Sezioni Unite.

3) intercettazioni ambientali disposte con captatore informatico all'interno dei luoghi di cui all'art. 614 c.p., solamente nel caso in cui vi sia un fondato motivo di ritenere che all'interno si stia svolgendo l'attività criminosa, qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini dello svolgimento delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20.

4.2. Il dispositivo elettronico portatile.

Sempre in linea con quanto previsto dalla legge delega, il Governo ha stabilito che la peculiare modalità captativa possa avvenire esclusivamente con l'inoculazione del virus *trojan* «anche» in un dispositivo elettronico *target* dotato del carattere della "portabilità" («dispositivo elettronico portatile» art. 266, comma 2, primo periodo c.p.p.)[100].

In primo luogo si nota come vi sia la possibilità che sul concetto di "dispositivo elettronico portatile" si apra un nutrito dibattito in sede giurisprudenziale e dottrinale, dal momento che vi sono alcuni dispositivi che si situano in una "zona grigia" tra la nozione di portatile e di fisso. Si pensi, per fare un esempio, a un *laptop*, eventualmente con un malfunzionamento della batteria. Date le dimensioni e una libertà di locomozione certamente non agile, è possibile ricomprendere il detto dispositivo tra quelli portatili richiamati dalla norma? La risposta a una simile domanda, che potrebbe valere anche per altri oggetti di uso quotidiano, veicola il regime di utilizzabilità dibattimentale dell'intercettazione itinerante.

La scelta legislativa che, a prima vista, sembra circoscrivere l'intercettazione virale ai soli dispositivi portatili non convince. Come noto, infatti, qualsiasi apparecchiatura dotata di una connessione internet può essere infettata dal *trojan horse* e, come tale, essere il veicolo per le intercettazioni di comunicazioni e conversazioni tra presenti (si pensi, tra gli altri, ai PC fissi dotati di microfono e videocamera, alle televisioni *smart*, ma anche alle telecamere di sicurezza). Può accadere, e nella pratica si verifica, che gli investigatori abbiano il fondato motivo di ritenere che all'interno di un determinato luogo si stia svolgendo l'attività criminosa, ma che, al contempo, non sia ancora iscritto nel registro degli indagati alcun soggetto: in tali casi, non vi è la possibilità per la Procura della Repubblica di disporre l'intercettazione ambientale con la tecnologia *de qua* – sebbene possa essere indispensabile ai fini della prosecuzione delle indagini – ma solamente con i mezzi "tradizionali", ossia con il posizionamento di un dispositivo captativo (c.d. cimice) fisicamente all'interno del luogo oggetto di indagine. Non può revocarsi in dubbio che una simile operazione possa comportare gravi rischi per l'incolumità degli ufficiali e agenti di PG deputati ad espletare tale incombente, nonché

[100] L'emendamento n. 36.4000 al ddl s. 2067 citato da F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., p. 355, prevedeva di disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in «dispositivi informatici e telematici», anziché in «dispositivi elettronici portatili».

per la segretezza delle indagini, i quali avrebbero potuto essere annullati laddove il legislatore avesse disciplinato anche certe situazioni.

Vi è di più. Se il legislatore avesse disciplinato la materia come sopra auspicato, non sarebbe certamente venuto meno all'idea riformatrice di tutela della riservatezza per almeno due ordini di ragioni. In primo luogo, un'intercettazione captativa itinerante si inserisce con forza lesiva maggiore nella sfera privata del soggetto rispetto a un'intercettazione tradizionale. In secondo luogo, se vi è il fondato motivo di ritenere che all'interno di un determinato luogo – anche di privata dimora – si stia svolgendo un'attività criminosa, l'intercettazione ambientale può in ogni caso essere disposta e il risultato a cui si perviene è il medesimo: l'acquisizione di tutto ciò che viene ascoltato all'interno del locale. L'unica differenza è il mezzo con il quale l'intercettazione viene effettuata. In altre parole, medesimi sono i risultati, medesimo è il livello di lesione della riservatezza dei soggetti che frequentano il luogo destinatario della captazione, differente è la modalità captativa: si è in presenza di una illogicità normativa riscontrabile *ictu oculi*.

A una soluzione analoga si può giungere anche in presenza di un'indagine per uno dei reati elencati nell'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., con l'unica differenza che non è necessario il *fumus perdurantis criminis* all'interno dei luoghi di privata dimora di cui all'art. 614 c.p.

Al fine di evitare illogicità sistemiche – nonostante la relazione di accompagnamento al decreto legislativo in commento sia chiara nel sostenere che il delegante ha inteso limitare «l'ambito dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inoculazione di dispositivo portatile e non anche di dispositivi fissi»[101] – sembra possibile fornire un'interpretazione adeguatrice del rinnovato apparato codicistico e ammettere le intercettazioni virali (non itineranti) anche se effettuate ai danni di un dispositivo fisso installato (anche) in un luogo di privata dimora, a condizione che, in questo ultimo caso, vi sia il fondato motivo di ritenere che ivi si stia svolgendo un'attività criminosa o che si proceda per uno dei gravi delitti di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.

In primo luogo, sarebbe irragionevole ritenere che se è possibile installare una microspia in un determinato luogo, al fine di captare tutte le comunicazioni che avvengono all'interno del "raggio di portata" della cimice (che peraltro rimane accesa tutto il giorno), al medesimo risultato non si possa giungere tramite un'agevole inoculazione di un virus informatico da remoto in un dispositivo elettronico fisso, stante la facile indicazione nel decreto autorizzativo del luogo in cui si trova l'apparecchio da sottoporre a monitoraggio virale.

Inoltre, stante la natura fissa del dispositivo, non vi sarebbe il rischio che questo venga trasportato in altro posto e compiere di conseguenza una intercettazione itinerante: si rimarrebbe, in altre parole, nel solco tracciato da una intercettazione ambientale "tradizionale", solamente effettuata con l'ausilio di un mezzo tecnico avanguardistico.

---

[101] C.D.M., *D.lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 9.

Infine, la *littera legis* non sembra essere, ad una lettura approfondita, ostativa all'intercettazione ambientale-virale non itinerante. Invero, l'art. 266, comma 2, c.p.p. consente l'intercettazione itinerante «*anche* mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile». Ed è proprio la congiunzione "anche" sembra essere semplicemente il riconoscimento di una intercettazione i cui contorni spaziali non sono definibili (quantomeno con termini di certezza) a priori; mentre qualora il luogo sia ben definito e circoscritto, se è possibile installare una cimice allora deve ritenersi praticabile, qualora vi sia un dispositivo fisso adatto, l'inoculazione di un virus informatico al solo fine intercettivo-ambientale non itinerante. Non ostativo, peraltro, sembra anche l'art. 267, comma 1, secondo periodo, c.p.p. che si richiede un onere motivazionale aggiunto del giudice per le indagini preliminari, dal momento che il periodo in questione si riferisce esclusivamente all'utilizzo del captatore informatico a fini intercettivo-itineranti su di un dispositivo elettronico portatile[102].

4.3. La funzione di audio-captazione.

Il legislatore delegante, oltre a voler circoscrivere la funzione captativa del virus informatico alle sole intercettazioni itineranti – sebbene si ritenga in via interpretativa di poter ammettere l'utilizzabilità della funzione di "intercettazione ambientale statica" del virus *trojan* – ha altresì palesato la volontà di delimitare ulteriormente la captazione alla sola registrazione audio. Tale volontà traspare nitidamente nell' art. 1, comma 84, lett. *e*, n. 1, l. 103/2017[103], il quale prescrive che «l'*attivazione del microfono* avvenga solo in conseguenza di apposito comando inviato da remoto»[104]; nonché nell' art. 1, comma 84, lett. *e*, n. 2, l. 103/2017, che si riferisce espressamente alla «*registrazione audio*» che deve essere avviata dalla polizia giudiziaria. Il legislatore delegato, dal canto suo, consapevole delle ulteriori potenzialità del captatore informatico non prese in considerazione dal parlamento[105], traduce in legge il suddetto criterio direttivo all'art. 267, comma 1, c.p.p.,

---

[102] In dottrina v. D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 217, secondo cui «nessun problema si pone nel caso di infezione di un dispositivo non portatile posto che l'attivazione del microfono garantisce comunque la sicura determinabilità del luogo in cui avvengono le captazioni. Diversa è la questione nel caso di apparati che, in ragione della loro portabilità, consentono intercettazioni ubiquitarie».

[103] Critica al riguardo D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 400. Secondo l'Autore la legge delega avrebbe imposto al legislatore delegato un principio direttivo di non facile attuazione pratica, dal momento che risulterebbe «assai improbabile e inverosimile» che la polizia giudiziaria possa procedere a un monitoraggio costante del soggetto bersaglio, attivando e disattivando il microfono nel corso di tutta la giornata; senza contare, peraltro, l'ingente dispendio di personale da adibire alle dette operazioni.

[104] «Si tratta di una previsione in linea con il principio di proporzionalità, dato che consente di attivare il microfono solo quando necessario» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 246).

[105] «Si tratta dunque di un complesso di operazioni (alcune delle quali già praticate ove consentite dalla legislazione vigente) che la tecnologia consente di effettuare, ma che il delegante non ha inteso regolare, limitando l'ambito dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inoculazione di dispositivo portatile (*smartphone, tablet* ecc.) e non anche dispositivi fissi» (C.D.M., *D.lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 9).

ove impone di indicare nel decreto autorizzativo giudiziale i luoghi e il tempo «in relazione ai quali è consentita l'attivazione del *microfono*»[106].

Il chiaro tenore letterale della norma, quindi, sembra escludere in ogni caso la possibilità di effettuare video riprese di comportamenti comunicativi: a differenza di quanto previsto in tema di intercettazioni "tradizionali", che si riferiscono semplicemente a intercettazioni di comunicazioni e conversazioni, l'art. 267, comma 1, c.p.p., imponendo i tempi e i luoghi di attivazione del microfono pare escludere *ex ante* la possibilità di utilizzare un tale strumento.

Quid iuris, però, se aderendo all'opinione sopra esposta, secondo la quale è possibile procedere a un'intercettazione ambientale fissa con il captatore informatico, mediante l'utilizzo di quest'ultimo strumento inoculato in un dispositivo fisso si effettuassero non solo audio registrazioni, bensì anche riprese visive di comportamenti comunicativi? Pare essere di fronte al medesimo problema interpretativo (scaturito prima della e) risolto dalla sentenza delle Sezioni Unite Prisco[107], chiamata a sciogliere la *quaestio iuris* inerente alla possibilità di intercettare comunicazioni domiciliari *inter praesentes* con strumenti di videoripresa anziché di ripresa sonora, dal momento che le telecamere finivano e «finiscono inevitabilmente per riprendere anche comportamenti domiciliari di tipo non comunicativo, ossia per realizzare una violazione sensoriale del domicilio non regolata dalla legge»[108]. Al riguardo la Corte di Cassazione ha ritenuto legittima la pratica di effettuazione di videoriprese, precisando però che il giudice a posteriori deve vagliare se quanto ripreso rappresenti un comportamento comunicativo[109] – in quanto tale riconducibile al paradigma intercettivo – ovvero non comunicativo, poiché in tale ultimo caso il materiale cognitivo è da ritenere inutilizzabile in giudizio.

Con la recente riforma si è di fronte al medesimo problema, con l'unica differenza che risiede nella protasi del paradigma ipotetico: se si ritiene possibile ricorrere all'intercettazione con captatore informatico effettuando audio registrazioni ambientali-fisse, allora è possibile utilizzare il medesimo strumento finanche per le riprese visive di comportamenti comunicativi? Secondo condivisibile opinione dottrinale, è d'uopo effettuare un rimando alla disciplina generale sul tema «e, nello specifico, ai principi enucleati da Cass., SS.UU., sentenza n. 26795/2006 che ha ribadito il divieto delle riprese

---

[106] Come correttamente osservato in dottrina, «la necessità di sganciare la procedura di installazione del captatore dall'effettiva ed autonoma attivazione del microfono dell'apparecchio di destinazione può soltanto dedursi implicitamente dal riferimento contenuto nel nuovo art. 267, co. 1 c.p.p.» (L. SURACI, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni: qualche rilievo critico*, in *www.pluris-cedam.utetgiuridica.it*, 05 gennaio 2018, p. 5).

[107] Cass., Sez. Un., 28 luglio 2006, n. 26795, Prisco.

[108] F. CAPRIOLI, *Il "captatore informatico"*, op. cit., p. 500.

[109] Per la nozione di comportamento non comunicativo v. Cass., Sez. VI, 10 novembre 1997, n. 4397, secondo cui «la nozione di comunicazione consiste nello scambio di messaggi fra più soggetti, in qualsiasi modo realizzati (ad esempio, tramite colloquio orale o anche gestuale) […] L'attività di intercettazione è appunto diretta a captare tali messaggi […] Attività del tutto differente dall'usuale azione intercettiva sopra descritta, è quella di "captare immagini relative alla mera presenza di cose o persone o ai loro movimenti, non funzionali alla captazione di messaggi».

visive di comportamenti non comunicativi avvenuti in ambito disciplinare»[110], con la precisazione, però, che le operazioni di video ripresa non potranno essere effettuate nel caso in cui si proceda a un'intercettazione captativa-itinerante.

4.4. La procedura autorizzativa.

Come visto in precedenza[111], al giudice per le indagini preliminari è richiesto un rafforzato onere motivazionale nel caso in cui debba autorizzare un'intercettazione virale-itinerante, comportante non solo la già descritta indicazione del tempo e del luogo ove è consentita l'attivazione del microfono, bensì anche «le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini» (art. 267, comma 1, c.p.p.).

La motivazione in ordine alle ragioni di necessarietà dell'agente intrusore, in ogni caso, non deve essere considerata in «termini assoluti»[112], dal momento che non si devono confondere il piano dei presupposti dell'attività intercettiva con quello dei presupposti applicativi dello strumento virale. Invero, questo secondo piano si riferisce semplicemente alle modalità esecutive[113] dell'intercettazione, la quale comunque deve possedere i requisiti generali dell'assoluta indispensabilità ai fini della prosecuzione delle indagini ovvero della necessarietà per lo svolgimento delle stesse, rispettivamente se si procede per un delitto comune o uno di criminalità organizzata a cui si applica la disciplina derogatoria di cui all'art. 13 d.l. 152/1991[114]. Inoltre, l'utilizzo del termine «necessarietà» – utilizzato dall'art. 267, comma 1, c.p.p. – indica già di per sé un *quid minus* rispetto alla «assoluta indispensabilità» richiesta dal secondo periodo del secondo comma del medesimo articolo. Ragionando in termini differenti verosimilmente si finirebbe con il gravare il giudice di uno sforzo motivazionale talmente ingente da rendere quasi impossibile procedere con il peculiare strumento captativo itinerante: deve dunque ritenersi che «non sarà comunque necessaria la prova del fatto che il ricorso a tale peculiare forma di intercettazione sia l'unico strumento operativo praticabile»[115].

Vi possono comunque essere dei casi in cui è impossibile attendere il provvedimento autorizzativo del giudice per le indagini preliminari che potrebbe giungere in un momento in cui si è già verificato un pregiudizio per le indagini. Il

---

[110] F. PRETE, *Linee guida sulla nuova disciplina in tema di intercettazioni*, op. cit., p. 24.

[111] V. *supra* §4.1.

[112] C. GITTARDI, *Linee guida*, op. cit., p. 24.

[113] In dottrina si è evidenziato che, sebbene l'intercettazione itinerante sia una modalità attuativa dell'intercettazione tradizionale, essa comunque non può essere utilizzata se non in presenza di specifiche necessità: «se ne deduce che, per espressa *voluntas legis*, l'intercettazione mediante captatore informatico non rappresenta esclusivamente una delle varie ma equivalenti forme tra le alternative a disposizione della pubblica accusa, quanto piuttosto un mezzo che, per la particolare intrusività nella sfera di riservatezza del destinatario della captazione, richiede l'individuazione di specifiche necessità operative che rendano appunto manifesta una più agevole riuscita dell'operazione tramite l'inoculazione del c.d. virus di Stato sul bersaglio portatile» (D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 219).

[114] Sul punto v. C. GITTARDI, *Linee guida*, op. cit., p. 24.

[115] D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 219.

legislatore, quindi, con una disposizione «francamente irragionevole»[116] e che «desta perplessità»[117], ha introdotto nell'ordinamento il nuovo comma 2 *bis* dell'art. 267 c.p.p, in forze del quale il pubblico ministero può disporre l'intercettazione itinerante in casi di urgenza solamente se procede per uno dei delitti indicati all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., con l'onere motivazionale aggiunto di indicare le ragioni di urgenza per le quali è impossibile attendere il provvedimento giudiziale.

La disposizione in esame ha suscitato le critiche dei primi commentatori che ne ravvisano profili di incostituzionalità per violazione quantomeno dell'art. 3 Cost. Questi, infatti, ritengono che si è in presenza di una «iniqua disparità di disciplina»[118], sia perché non vi sarebbe alcuna ragione per differenziare il trattamento tra reati "ordinari" e reati di criminalità organizzata o terroristica, sia perché in ogni caso al giudice per le indagini preliminari è rimesso un controllo successivo sui presupposti del decreto d'urgenza[119].

Un ulteriore profilo di illegittimità costituzionale potrebbe rinvenirsi nella violazione dell'art. 76 Cost. per eccesso di delega. Invero, vi è una discrasia tra i principi direttivi del delegante e quanto effettivamente trasposto in legge dal delegato[120], dal momento che l'art. 267, comma 2 *bis*, c.p.p. impone al PM di indicare «le ragioni di urgenza» che rendono impossibile attendere l'autorizzazione del giudice; al contrario, la legge delega poneva in capo al pubblico ministero un doppio onere motivazionale ben più stringente, consistente nell'indicazione: 1) delle «specifiche situazioni di fatto che rendono impossibile la richiesta al giudice» e 2) delle «ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini».

In seguito alla decretazione d'urgenza, il pubblico ministero dovrà richiedere la convalida al gip con le modalità e gli effetti di cui all'art. 267, comma 2, c.p.p., ossia dovrà trasmettere immediatamente a quest'ultimo – e comunque non oltre 24 ore – il decreto con il quale ha disposto l'intercettazione itinerante. Il giudice è tenuto a decidere entro 48 ore dalla ricezione dalla comunicazione e, nel caso di mancata convalida, l'intercettazione non potrà essere proseguita e i risultati raccolti sino a quel momento saranno inutilizzabili. Anche in questo caso vi è una discrasia tra i principi e criteri direttivi della legge delega e quanto tradotto nel d.lgs. 216/2017. L'art. 1, comma 84, lett. *e*, n. 6, l. 103/2017 stabilisce infatti che la convalida giudiziale debba intervenire «entro il termine massimo di quarantotto ore»; al contrario, il rinvio operato dal comma 2 *bis* dell'art. 267 c.p.p. al comma 2 del medesimo articolo dilata a settantadue ore il termine massimo in cui è atteso il provvedimento del gip: al pubblico ministero sono concesse ventiquattro ore di tempo per comunicare al giudice per le indagini preliminari la disposizione dell'intercettazione d'urgenza; alle quali devono aggiungersi le quarantotto ore concesse a quest'ultimo per la decisione finale[121].

---

[116] D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 223.
[117] C. GITTARDI, *Linee guida*, op. cit., p. 25.
[118] D. PRETTI, *Prime riflessioni a margine*, op. cit., p. 223.
[119] C. GITTARDI, *Linee guida*, op. cit., p. 25.
[120] Così L. SURACI, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni*, op. cit., p. 6.
[121] Secondo parte della dottrina, anche in questo caso è ravvisabile «un ulteriore profilo di contrasto» costituzionale tra la legge delega e il decreto delegato (L. SURACI, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni*, op. cit., p. 6).

4.5. Le cause di inutilizzabilità dell'intercettazione captativa-itinerante.

Il legislatore ha tracciato il solco delle cause di inutilizzabilità dei risultati intercettivi itineranti, non senza allontanarsi in alcuni punti da quanto indicato dai criteri direttivi della legge delega, che possono essere così riassunte:

1) mancata osservanza delle disposizioni dettate dall'art. 267 c.p.p.: in questa sede rileva particolarmente la mancata indicazione nel decreto autorizzativo del giudice per le indagini preliminari delle ragioni di necessità della procedura captativa e dell'indicazione spazio-temporale della stessa[122] (art. 271, comma 1, c.p.p.);
2) mancata osservanza delle disposizioni di cui all'art. 268, commi 1 e 3, c.p.p., i quali prescrivono rispettivamente la necessaria redazione del verbale delle operazioni compiute e la possibilità operativa di ricorrere a impianti esterni alle procure della Repubblica solo per eccezionali ragioni di urgenza (art. 271, comma 1, c.p.p.);
3) inutilizzabilità dei dati acquisiti «nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile (art. 271, comma 1 *bis*, c.p.p.);
4) inutilizzabilità dei dati acquisiti «al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo» (art. 271, comma 1 *bis*, c.p.p.);
5) inutilizzabilità delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile «per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione», fatta salva l'indispensabilità per l'accertamento di delitti per i quali è previsto l'arresto obbligatorio in flagranza (art. 270, comma 1 *bis*, c.p.p.).

4.5.1. Il divieto di utilizzazione per "la prova di reati diversi".

Il legislatore ha inteso impedire la circolazione extraprocedimentale dei risultati investigativi ottenuti con l'agente intrusore inoculato su dispositivo elettronico portatile «per la prova di reati diversi per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza» (art. 270, comma 1 *bis*, c.p.p.). In tal modo il governo ha dato seguito, non senza alcune imprecisioni, alla delega parlamentare che imponeva, all'art. 1, comma 84, lett. *e*, n. 7, l. 103/2017, che «i risultati intercettativi così ottenuti po[tesser]o essere utilizzati ai fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e po[tesser]o essere utilizzati in procedimenti diversi a condizione che

[122] Sul punto si rinvia *supra* §4.1.

siano indispensabili per l'accertamento dei delitti di cui all'articolo 380 del codice di procedura penale»[123].

In primo luogo, si può notare come il criterio direttivo che imponeva al governo di consentire l'utilizzabilità delle risultanze investigative indispensabili per l'accertamento di uno dei reati annoverati nell'art. 380 c.p.p. sia stato in parte travisato e tradotto in legge con la locuzione «arresto obbligatorio in flagranza». Ora, è ben vero che i casi di cui all'art. 380 c.p.p. rappresentano ipotesi in cui è obbligatorio procedere all'arresto di un soggetto che si trovi in stato di flagranza, tuttavia non è vero il contrario: tale disposizione, infatti, non esaurisce i casi di obbligatorietà dell'arresto in flagranza, che si rinvengono anche in alcune discipline extracodicistiche[124]. Si pensi, anzitutto, all'art. 13, comma 13 *ter*, d.lgs. 25 luglio 1998, n. 286, ai sensi del quale è obbligatorio l'arresto (anche fuori dei casi di flagranza) dell'autore dei reati di reingresso abusivo nel territorio dello Stato, puniti con una pena edittale che varia da un minimo di un anno a un massimo di cinque anni di reclusione[125]. In secondo luogo, si evidenziano gli artt. 235, comma 3, e 312, comma 2, c.p., i quali dispongono l'arresto obbligatorio, anche fuori dei casi di flagranza, del responsabile dei reati di trasgressore agli ordini di espulsione o allontanamento dallo Stato da essi rispettivamente previsti[126].

Inoltre, come si evince dalla formulazione letterale della norma, il legislatore, impedendo la circolazione esoprocedimentale degli atti investigativi «per la prova di reati diversi», ha voluto – sul tema dell'intercettazione itinerante – porre un freno al diritto vivente che si era creato sotto la vigenza dell'art. 270, comma 1, c.p.p.[127]. Invero, la giurisprudenza costante è giunta a sostenere che la nozione di «diverso procedimento» non debba essere intesa in senso formalistico, dal momento che «il concetto di "diverso procedimento" nel quale, ai sensi dell'art. 270 c.p.p., comma 1, è vietata l'utilizzazione dei risultati delle intercettazioni di conversazioni o comunicazioni (salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio

---

[123] Secondo parte della dottrina «tale formulazione aveva suscitato qualche perplessità, soprattutto in riferimento alla prima statuizione, poiché l'attuazione di tale criterio avrebbe potuto determinare un doppio binario in tema di inutilizzabilità» (T. ALESCI, *Le intrusioni* inter praesentes, op. cit., p. 83). Preoccupazioni che si sono poi in effetti rivelate fondate, se si tiene in considerazione che i risultati intercettivi ubiquitari non possono essere utilizzati per la prova di reati di diversi e non, come prescrive l'art. 270, comma 1, c.p.p., in procedimento diversi.

[124] Attenta dottrina ha osservato che la legge delega imponeva l'utilizzabilità delle risultanze intercettive per i reati di cui all'art. 380 c.p.p., mentre il decreto legislativo, uniformandosi all'art. 270, comma 1, c.p.p., ha tradotto il predetto riferimento con «arresto obbligatorio in flagranza» (L. SURACI, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni*, op. cit., p. 5).

[125] Il codice di rito, dal canto suo, prevede l'arresto obbligatorio in flagranza in caso di violazione dell'art. 12, commi 1 e 2, d.lgs. 286/1998, che puniscono «delitti di promozione, direzione, organizzazione, finanziamento o effettuazione di trasporto di persone ai fini dell'ingresso illegale nel territorio dello Stato» (art. 380, comma 2, lett. *m-ter*, c.p.p.).

[126] Per i detti reati, infatti, è prevista la pena edittale nel minimo di un anno e nel massimo di quattro anni di reclusione.

[127] Secondo F. PRETE, *Linee guida sulla nuova disciplina in tema di intercettazioni*, op. cit., p. 26, la differenza semantica «lascia intendere un ambito di utilizzabilità minore per le intercettazioni tra presenti mediante captatore informatico». Dello stesso avviso anche L. SURACI, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni*, op. cit., p. 6 e F. RUGGIERI, *L'impatto delle nuove tecnologie*, op. cit., p. 369.

l'arresto in flagranza), non equivale infatti a quello di "diverso reato" ed in esso non rientrano pertanto, le indagini strettamente connesse e collegate sotto il profilo oggettivo, probatorio e finalistico al reato in ordine al quale il mezzo di ricerca della prova è stato disposto»[128].

Ad oggi, quindi, i dati acquisiti con l'intercettazione itinerante potranno essere utilizzati esclusivamente per la prova del reato per il quale è stata disposta e non, invece, in procedimento diversi. Questa, sebbene per parte della dottrina sia «solo in parte comprensibile»[129] e segni un «ingiustificato doppio binario»[130], pare essere l'unica esegesi praticabile della norma: diversamente opinando, infatti, il comma 1 *bis de quo* risulterebbe essere tautologico e una mera superfetazione normativa se raffrontato al comma che precede[131], privando così di autonomo significato precettivo la disposizione[132].

In ogni caso, così come nel vigore della previgente disciplina, i risultati investigativi inutilizzabili possono assumere valora di *notitia cirminis*[133-134].

5. Conclusioni.

In conclusione non si può non notare l'occasione mancata del legislatore nel disciplinare le proteiformi potenzialità tecniche dell'agente intrusore, limitandosi a dar seguito al diritto pretorio che si era creato in relazione alle intercettazioni tra presenti[135].

---

[128] Cass., Sez. III, 28 febbraio 2018, n. 28516. V. anche Cass., Sez. III, 21 gennaio 2016, n. 2608, in; Cass., Sez. Un., 26 giugno 2014, n. 32697.

[129] C. GITTARDI, *Linee guida*, op. cit., p. 29.

[130] L. PALMIERI, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni*, in *Dir. pen. cont. – Riv. trim.*, 1/2018, p. 64.

[131] L'art. 270 comma 1 c.p.p., infatti, tratta del *genus* intercettazioni, che per forza di cose ricomprende anche la *species* intercettazioni mediante l'utilizzo di captatore informatico.

[132] In ogni caso, vi potrebbero essere profili di illegittimità costituzionale dell'art. 270, comma 1 *bis*, c.p.p. per violazione dell'art. 76 Cost. L'art. 1, comma 84, lett. *e*, n. 7, l. 103/2017, infatti, consente l'utilizzabilità delle risultanze intercettive a fini di prova nel procedimento per il quale sono state disposte (e diversamente non potrebbe essere), mentre ammette la possibilità della loro utilizzazione in *procedimenti* diversi, non – come legiferato dal Governo – per *reati* diversi. Un netto contrasto, quindi, tra i criteri direttivi del Parlamento e la trasposizione in legge del Governo.

[133] Così C. GITTARDI, *Linee guida*, op. cit., p. 30. V. anche D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 409, la quale definisce un «paradosso» che i risultati intercettivi inutilizzabili possano essere assunti quale notizia di reato.

[134] Secondo parte della dottrina «ad ogni modo, è intuibile che la "clausola generale di chiusura" inserita del comma 1 *bis* dell'art. 270 c.p.p. "salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza" ha deluso le aspettative della dottrina che attendeva dal Legislatore un segnale di discontinuità rispetto alla giurisprudenza orientata al "recupero" del materiale probatorio» (L. PALMIERI, *La nuova disciplina del captatore informatico*, op. cit., p. 64).

[135] Secondo M. TORRE, *Il captatore informatico nella legge delega 23 giugno 2017, n. 103*, op. cit., p. 442, la delega Orlando (e la conseguente riforma) «lascia insoddisfatti», dal momento che non è stato possibile disciplinare compiutamente, da un punto di vista giuridico, la poliedricità funzionale dell'agente intrusore. Dello stesso avviso anche S. SIGNORATO, *Le indagini digitali*, op. cit., p. 241.

Più ambizioso, quindi, sarebbe stato discutere ed approvare il d.d.l. Quintarelli («Disciplina dell'uso di captatori legali nel rispetto delle garanzie individuali») presentato a inizio 2017, dopo un anno di gestazione da parte di tecnici e giuristi, il quale si pone l'obiettivo di "segmentare" le funzionalità degli strumenti di osservazione e acquisizioni da remoto, ascrivendo (1) a nuovo mezzo di ricerca della prova la ricerca di *file* su dispositivo; (2) alle intercettazioni telefoniche le intercettazioni del traffico vocale; infine (3) alle intercettazioni tra presenti le audio e video registrazioni, così abbracciando a tutto tondo (o quasi) le potenzialità del captatore informatico[136].

[136] Dello stesso avviso D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, op. cit., p. 388 s. In ogni caso, emerge «l'urgente necessità di elaborare istituti nuovi, che prescindano dall'ancoraggio al requisito della materialità e tengano conto [non solo] delle specificità delle indagini digitali» (S. SIGNORATO, *Le indagini digitali*, op. cit., p. 124), ma anche delle poliedriche potenzialità tecniche di cui uno strumento come il captatore informatico è permeato.